

METHOD AND DEVICE FOR TRANSMITTING RECEIVING DATA

Publication number: JP10269290

Publication date: 1998-10-09

Inventor: MAARI KOUICHI; FUKAMI TAKESHI

Applicant: SONY CORP

Classification:

- international: G06F7/58; B65G61/00; G06F9/06; G06F15/00; G06F19/00; G06F21/20; G06F21/22; G06Q10/00; G06Q20/00; G06Q30/00; G06Q50/00; H04L9/32; H04L29/08; G06F9/06; G06F7/58; B65G61/00; G06F9/06; G06F15/00; G06F19/00; G06F21/20; G06F21/22; G06Q10/00; G06Q20/00; G06Q30/00; G06Q50/00; H04L9/32; H04L29/08; G06F9/06; (IPC1-7): G06F9/06; G06F17/60; G06F7/58; G06F15/00; G06F19/00; H04L9/32; H04L29/08

- European:

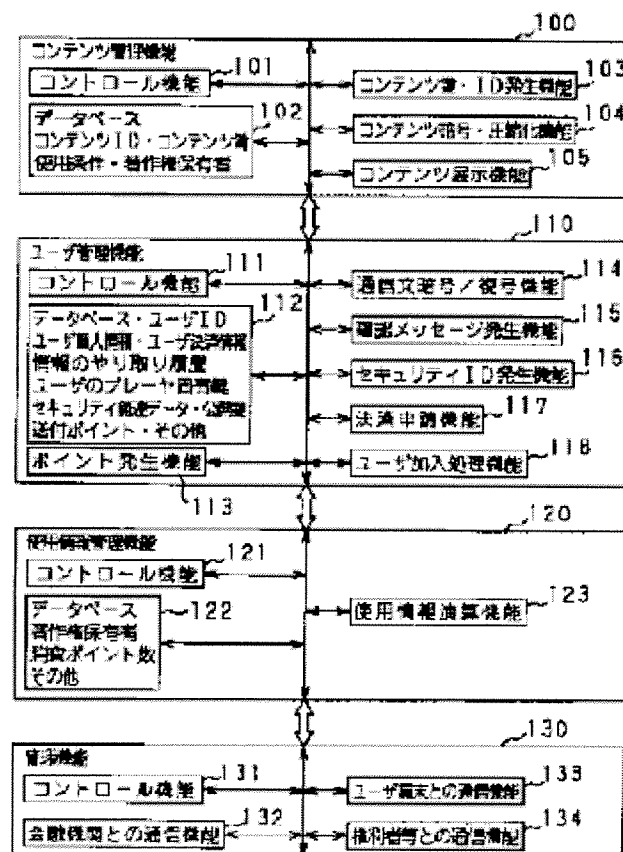
Application number: JP19970074183 19970326

Priority number(s): JP19970074183 19970326

Report a data error here

Abstract of JP10269290

PROBLEM TO BE SOLVED: To make it possible to prevent what is called 'disguise' at the time of the communications of simple money amount replenishing data, by comparing a random number added to reception data with a random number generated by itself and treating reception data as the right one only at the time of coincidence. **SOLUTION:** A user management function block 110 calculates new security ID to the player based on random number generation in a security ID generating function part 115 and, moreover, a control function part 111 enciphers security ID together with point information. Enciphering at this time is also executed by using a session key, which is previously transmitted from the player. Thus, the random number is generated whenever data exchange is executed with a communication opposite party, the random number is added to transmission data at the time of transmitting data, the random number added to reception data is compared with the one generated at this side in a data reception side and, then, reception data is treated as the right one only at the time of coincidence.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-269290

(43) 公開日 平成10年(1998)10月9日

(51) Int.Cl. ⁶	識別記号	F I
G 0 6 F 17/60		G 0 6 F 15/21 3 3 0
7/58		7/58 B
15/00	3 3 0	15/00 3 3 0 C
19/00		9/06 5 5 0 Z
H 0 4 L 9/32		15/30 L

審査請求 未請求 請求項の数 8 O L (全 36 頁) 最終頁に続く

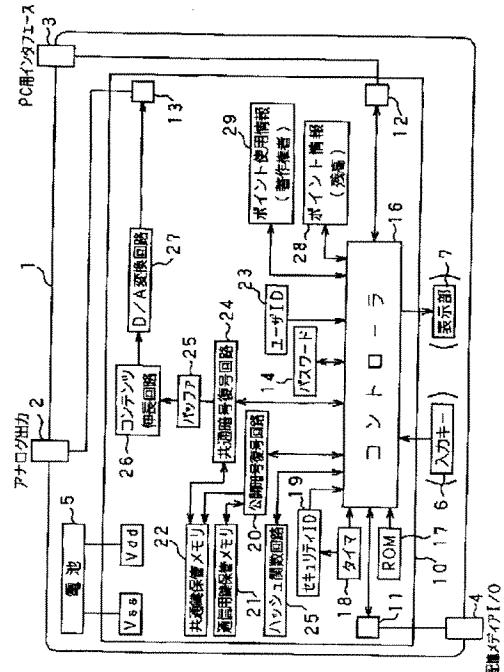
(21) 出願番号	特願平9-74183	(71) 出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22) 出願日	平成9年(1997)3月26日	(72) 発明者	真有 浩一 東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(72) 発明者	深海 武 東京都品川区北品川6丁目7番35号 ソニー株式会社内
		(74) 代理人	弁理士 小池 晃 (外2名)

(54) 【発明の名称】 データ送受信方法及び装置

(57) 【要約】

【課題】 単純な金額補充データの通信の際のいわゆる「成り済まし」を防ぐことを可能にする。

【解決手段】 通信相手側との間でデータ送受信を行う毎に乱数としてのセキュリティIDを発生するセキュリティID発生回路19及びタイマ18と、データ送信を行うときには送信データにセキュリティIDを付加して送信し、データ受信を行ったときには通信相手側から送信されてきたデータに付加されたセキュリティIDと自己が発生したセキュリティIDとを比較して一致したときのみ、その受信データを正当なものとして扱うコントローラ16とを有する。



【特許請求の範囲】

【請求項1】 通信相手側との間でデータ送受信を行う毎に乱数を発生し、

データ送信側ではデータに上記乱数を付加して送信し、データ受信側では上記データ送信側から送信されてきたデータに付加された乱数と自己が発生した乱数とを比較し、上記比較において一致したときのみ上記受信したデータを正当なものとして扱うことを特徴とするデータ送受信方法。

【請求項2】 上記送受信されるデータは金額データであることを特徴とする請求項1記載のデータ送受信方法。

【請求項3】 上記金額データはプリペイド方式の金額補充データであることを特徴とする請求項1記載のデータ送受信方法。

【請求項4】 上記金額補充データは、暗号化及び圧縮されたデジタルコンテンツを復号する毎に減額される課金情報であることを特徴とする請求項3記載のデータ送受信方法。

【請求項5】 通信相手側との間でデータ送受信を行う毎に乱数を発生する乱数発生手段と、

データ送信を行うときには送信データに上記乱数を付加して送信するデータ送信手段と、

データ受信を行ったときには通信相手側から送信されてきたデータに付加された乱数と自己が発生した乱数とを比較し、上記比較において一致したときのみ上記受信したデータを正当なものとして扱うデータ受信手段とを有することを特徴とするデータ送受信装置。

【請求項6】 上記送受信されるデータは金額データであることを特徴とする請求項5記載のデータ送受信装置。

【請求項7】 上記金額データはプリペイド方式の金額補充データであることを特徴とする請求項5記載のデータ送受信装置。

【請求項8】 上記金額補充データは、暗号化及び圧縮されたデジタルコンテンツを復号する毎に減額される課金情報であることを特徴とする請求項7記載のデータ送受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、例えばデータの送受信を行うデータ送受信方法及び装置に関する。

【0002】

【従来の技術】コンピュータプログラムやオーディオデータ、ビデオデータ等のデジタルコンテンツの流通を簡便化し、潜在需要を掘り下げ、市場拡大に有利な手法としては、例えば特公平6-19707号公報に記載されるソフトウェア管理方式、特公平6-28030号公報に記載されるソフトウェア利用管理方式、特公平6-95302号公報に記載されるソフトウェア管理方式の

ような手法が存在する。上記特公平6-19707号公報に記載されたソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、ソフトウェアの利用状況をソフトウェア権利者別などによって把握できるようにしたものである。また、特公平6-28030号公報に記載されるソフトウェア利用管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムを買い取り（買い取った後は無料で使用できる）価格を付し、コンピュータシステム内には購入可能な金額を示すデータを設けておき、有償プログラム購入の際は、同システムにある利用可能なソフトウェアの名称としてテーブルに登録すると共に、当該購入可能金額を示すデータをソフトウェア価格分だけ減じ、また登録済みソフトウェアを該テーブルから抹消する際には状況に応じて該購入可能な金額を示すデータを増加更新するようにしたものである。また、上記特公平6-95302号公報に記載されるソフトウェア管理方式は、無体財産であるコンピュータプログラムやビデオデータ等のソフトウェアの利用に際し、有償プログラムにつき実際の利用量（利用回数または利用時間など）に応じて利用料金を徴収するために、利用されたプログラムの識別と「利用者識別符号と料金を記録」しておき、該記録を回収することでプログラム権利者が自分の所有するプログラムの利用料金を把握でき、プログラムの利用量に応じたプログラム利用料金を回収する場合のシステムで有効なものである。

【0003】

【発明が解決しようとする課題】ところで、従来より、電子商取引においては、小額決済の際に毎回金融機関を通して決済することによる手数料等の金額増加が問題視されている。その解決策の一つとしていわゆるプリペイド方式が提案されている。すなわちこのプリペイド方式では、予め任意の金額分を示す金額補充データ（以下、プリペイド情報と呼ぶ）を購入しておき、電子商取引を行う毎に、当該予め購入しておいたプリペイド情報から当該取引分に相当する額を減額する方式である。

【0004】また、前記公報記載のソフトウェア管理方式などの場合も、デジタルコンテンツを流通させる仕組みとして検討されているが、その問題点の一つとして、小額のコンテンツ代金を決済するのに必要なネットワーク使用料金が、当該コンテンツ代金に比べて無視できないことが指摘されている。これを解決するための方法の一つとしても上記プリペイド方式が提案されている。

【0005】しかし、上記プリペイド方式の場合、上記プリペイド情報を購入する度に、同じようなデータ（例えば暗号化された「3000円補充」というメッセージなど）のやりとりが行われることになる。このように、毎回同じようなデータのやり取りを行う場合、例えば悪

意を持つ者による金融機関へのいわゆる「成り済まし」による金額補充が問題点として指摘されている。なお、ここに言う金融機関への「成り済まし」とは、上記悪意を持った者が本来のユーザ（正当なユーザ）に成り済まして、不正にプリペイド情報を入手するようなことを言う。

【0006】すなわち、プリペイド情報の購入の度に、毎回同じようなデータのやり取りを行うと、悪意を持った者が当該データを通信回線から盗み出して同じデータを生成して、プリペイド情報の配信側にその情報の入手を依頼し、当該配信側からのプリペイド情報の送りを自分（悪意を持った者）にしたような場合、当該悪意を持った者がプリペイド情報を入手できることになり、さらにこのプリペイド情報の購入代金の請求は本来のユーザになされることになるという問題が発生するおそれがある。

【0007】そこで、本発明はこのような状況に鑑みてなされたものであり、単純な金額補充データの通信の際のいわゆる「成り済まし」を防ぐことを可能にするデジタルコンテンツ管理装置及び方法を提供することを目的とする。

【0008】

【課題を解決するための手段】本発明によれば、通信相手側との間でデータ送受信を行う毎に乱数を発生し、データ送信時には送信データに乱数を付加し、データ受信側では受信データに付加された乱数と自己が発生した乱数とを比較して一致したときのみ受信データを正当なものとして扱うことにより、上述した課題を解決する。

【0009】

【発明の実施の形態】以下、本発明の好ましい実施の形態について、図面を参照しながら説明する。

【0010】先ず、本発明のデータ送受信方法及び装置の具体的内容及び構成の説明を行う前に、これらの理解を容易にするために、本発明が適用されるシステム全体の概略構成及びシステムの運用方法について図1から図7までの各図を用いて簡単に説明する。

【0011】図1にはシステム全体の概略的な構成を示す。

【0012】この図1において、ユーザ側200は、本発明のデジタルコンテンツ再生装置（以下、プレーヤ1と呼ぶことにする）及びいわゆるパーソナルコンピュータ（以下、ユーザ端末50と呼ぶことにする）を保有しているものとする。

【0013】ユーザ端末50は、通常のパーソナルコンピュータであるが、本発明に使用する後述する各種ソフトウェアをアプリケーションソフトとして格納してなると共に、表示手段であるディスプレイ装置と放音手段であるスピーカ、及び情報入力手段であるキーボードやマウス等が接続されてなるものである。当該ユーザ端末50は例えばネットワークを介してシステム管理会社21

0と接続可能であり、また、プレーヤ1との間のインターフェイス手段を有し、データ送受が可能である。

【0014】プレーヤ1は例えば図2に示すような構成を有するものである。

【0015】この図2の構成の詳細な説明については後述するが、当該プレーヤ1は、デジタルコンテンツの処理経路の主要構成要素として、暗号化されているデジタルコンテンツをコンテンツ鍵を用いて復号化する共通鍵暗号復号回路24と、圧縮されているデジタルコンテンツを伸長する伸長手段である伸長回路26と、デジタルデータをアナログ信号に変換するD/A変換回路27とを少なくとも有する。なお、以下に言う復号化とは、暗号化を解くことである。

【0016】また、このプレーヤ1は、使用するデジタルコンテンツの権利情報及び使用状況を示す情報（以下、これら情報をポイント使用情報と呼ぶ）や、デジタルコンテンツを使用する際に必要となる保有金額データ、すなわちデジタルコンテンツを使用する毎に減額される課金データ（以下、ポイント情報と呼ぶ）等を扱う主要構成要素として、上記ポイント使用情報を格納するポイント使用情報格納メモリ29と、上記ポイント情報を格納するポイント情報格納メモリ28とを少なくとも備えている。

【0017】さらに、このプレーヤ1は、後述するような暗号化及び復号化に使用する各種鍵を格納するための構成として共通鍵保管メモリ22及び通信用鍵保管メモリ21と、これらに格納された鍵を用いて暗号化や復号化を行うための構成として共通暗号復号回路24及び公開暗号復号回路20を有している。また、このプレーヤ1は、上記暗号化及び復号化に関連する構成として、システム管理会社210のホストコンピュータと連動した乱数を発生してセキュリティIDを生成するセキュリティID発生回路19及びタイマ18や、後述するいわゆるハッシュ値を発生するハッシュ関数回路25等をも有している。

【0018】その他、当該プレーヤ1は、デジタルコンテンツやその他各種のデータ及び各構成要素の制御をROM17に格納されたプログラムに基づいて行う制御手段であるコントローラ16と、携帯時の動作電源としての電池5を備えている。

【0019】ここで、図2のプレーヤ1の各主要構成要素は、セキュリティ上、IC（集積回路）或いはLSI（大規模集積回路）の1チップで構成されることが望ましい。この図2では、各主要構成要素が集積回路10内に1チップ化されている。当該プレーヤ1には、外部とのインターフェイス用として3つの端子（アナログ出力端子2と、PC用インターフェイス端子3と、記録メディア用I/O端子4）を備え、これら各端子が集積回路10のそれぞれ対応する端子13、12、11に接続されている。なお、これら各端子は統合することも、また

新たに別の端子を設けることも可能であり、特にこだわるものではない。

【0020】システム管理会社210は、システム全体を管理する管理センタ211と、上記プレーヤ1を販売する販売店212とからなり、仮想店舗230を介してユーザ側200のユーザ端末50との間で、後述するようなデジタルコンテンツの供給に関する情報の送受、コンテンツプロバイダ240が保有するコンテンツを圧縮及び暗号化するデジタルコンテンツの加工、上記加工したデジタルコンテンツの供給、金融機関220との間の情報送受等を行う。なお、システム管理会社210と金融機関220との間では、ユーザ側200の口座番号やクレジット番号、名前や連絡先等の確認や、ユーザ側200との間で取引可能かどうかの情報等のやり取りなどが行われる。金融機関220とユーザ側200の間では、実際の代金振込等の処理が行われる。また、販売店212は、必ずしもシステム管理会社210内に含まれる必要はなく、販売代理店であってもよい。

【0021】上記システム管理会社210の管理センタ211は、例えば図3に示すような構成を有するものである。この図3の構成の詳細な説明については後述するが、主要構成要素として、デジタルコンテンツを管理し、その展示、暗号化及び圧縮等の加工処理、デジタルコンテンツの暗号化及び復号化に使用する鍵情報であるコンテンツ鍵やIDの発生等の各機能を有するコンテンツ管理機能ブロック100と、ユーザ情報を管理し、通信文（メッセージやポイント情報等）の暗号化及び復号化、確認メッセージの発生、セキュリティIDの発生、金融機関230との間での決済申請、ポイントの発生等の各機能の他、ユーザ加入処理等を行うユーザ加入処理機能部118をも備えたユーザ管理機能ブロック110と、ポイント使用情報等を管理する使用情報管理機能ブロック120と、システム全体を管理し、通信機能を有する管理機能ブロック130とを、少なくとも有してなる。

【0022】上述した図1のように構成されるシステムの実際の運用方法の一例を、図4～図7を用いて説明する。なお、以下の運用方法は、ユーザ側200やシステム管理会社210、金融機関220、コンテンツプロバイダ240等が実際に行う手順である。

【0023】このシステムの運用方法の説明では、プレーヤ1の購入の手順、デジタルコンテンツの検索からプレーヤ1用の記憶メディアに対するデジタルコンテンツのインストールまでの手順、当該デジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該デジタルコンテンツを使用した場合の精算の手順、デジタルコンテンツの鑑賞に伴ってユーザから徴収した課金代金の分配の手順について順番に説明する。

【0024】先ず、プレーヤ1の購入時の手順として

は、図4の(1)及び(5)に示すように、ユーザ側200が実際に店頭或いは通信販売等により、上記販売店212から上記プレーヤ1を購入する。

【0025】このとき、上記販売店212は、図4の(2)に示すように、上記プレーヤ1の販売時に上記ユーザ側200から提供された個人情報（名前や連絡先等）及び決済情報（銀行口座、クレジット番号等）と、上記販売したプレーヤ1固有の番号（プレーヤ固有鍵等を含む）とをシステム管理会社210の管理センタ211に登録する。

【0026】管理センタ211は、図4の(3)に示すように、金融機関220に対して、上記ユーザ側200から提供された口座番号やクレジット番号等の確認を行い、図4の(4)に示すように金融機関220から取引可能である旨の情報を得る。

【0027】次に、デジタルコンテンツの検索からプレーヤ1用の記憶メディアへのデジタルコンテンツのインストールまでの手順として、上記プレーヤ1を購入したユーザ側200は、当該プレーヤ1とのインターフェイス手段を備えたユーザ端末50を使って、図5の(1)に示すように、希望のデジタルコンテンツの検索、選択、編集、注文等を行う。このときの検索から注文までの処理は、ユーザ端末50がアプリケーションソフトとして格納している検索ソフトを用い、例えばネットワークを介して接続された仮想店舗230に対して行う。

【0028】仮想店舗230は、例えば管理センタ211がネットワーク上の仮想的に設けている店舗であり、この仮想店舗230には、例えば複数のコンテンツの内容を示す情報が展示されている。ユーザ側200は、仮想店舗230にて提供されているこれらの情報に基づいて、所望のコンテンツの注文を行うことになる。なお、仮想店舗230に展示されるコンテンツの内容を示す情報としては、例えばコンテンツが映画等のビデオデータである場合には当該映画等のタイトルや広告、当該映画中の1シーン等の映像などが考えられ、また、コンテンツがオーディオデータである場合は曲名やアーティスト名、当該曲の最初の数フレーズ（いわゆるイントロ）等が考えられる。したがって、ユーザ側200のユーザ端末50にて上記仮想店舗230をアクセスした場合には、当該ユーザ端末50上に上記仮想店舗230の複数のコンテンツの内容が仮想的に展示され、これら展示物の中から所望のものを選択することでコンテンツの注文が行われることになる。

【0029】上記ユーザ側200のユーザ端末50からデジタルコンテンツの注文等があったとき、上記仮想店舗230は、図5の(2)に示すように管理センタ211に対してデジタルコンテンツの供給依頼を行う。

【0030】当該デジタルコンテンツの供給依頼を受け取った管理センタ211は、コンテンツプロバイダ2

10

20

30

40

50

40に対して上記供給依頼のあったデジタルコンテンツの配給依頼を行う。これにより、当該コンテンツプロバイダ240は、図5の(4)に示すように上記配給依頼のあったデジタルコンテンツを管理センタ211に配給する。

【0031】管理センタ211は、上記コンテンツプロバイダ240から配給されたデジタルコンテンツに対して暗号化及び所定の圧縮方式を用いた圧縮を施すと共に、この圧縮及び暗号化されたデジタルコンテンツに対して、当該コンテンツのID(コンテンツID)とこのコンテンツの著作権者等の権利者情報と当該コンテンツを使用したときの課金額とコンテンツをユーザ側200に供給する仮想店舗名等を付加する。なお、コンテンツに対する課金額は、コンテンツプロバイダ240にて事前に決定される。

【0032】上記管理センタ211にて加工されたコンテンツは、図5の(5)に示すように、仮想店舗230に送られ、さらにこの仮想店舗230を介して、図5の(6)のようにユーザ側200のユーザ端末50に供給される。これにより、プレーヤ1には、上記ユーザ端末50からコンテンツが供給され、このコンテンツが当該プレーヤ1に格納されることになる。

【0033】なお、この図5に(2)～(5)までの流れについては、事前に行っておくことも可能である。すなわち、仮想店舗230には、上記複数のコンテンツの内容を示す情報を展示するだけでなく、これら展示に対応した上記加工されたデジタルコンテンツを予め用意しておくようにしても良い。

【0034】次に、上述のようにしてプレーヤ1にインストールされたデジタルコンテンツを使用可能にするための課金用のポイント情報の購入と当該デジタルコンテンツを使用した場合の精算の手順では、先ず、ユーザ端末50によってプレーヤ1に格納されているポイント情報の不足が確認されて、当該ユーザ端末50からポイント情報の補充要求がなされる。

【0035】このとき、図6の(1)のように、当該ユーザ端末50からは、プレーヤ1にて暗号化されたポイント情報の補充依頼が、管理センタ211に対し転送される。また同時に、既に使用したデジタルコンテンツに対応する著作権者等の権利者の情報すなわちポイント使用情報がプレーヤ1から読み出されて暗号化され、ユーザ端末50を介して管理センタ211に送られる。このように、ポイント情報の補充依頼と同時にポイント使用情報の転送が行われるようにしたのは、当該ポイント使用情報の管理センタ211への送信のみのために、ユーザ側200が管理センタ211にアクセスする手間を省くためである。勿論、このポイント使用情報の転送は、必ずしもポイント情報の購入と同時に進行する必要はなく、独立に行っても良い。

【0036】上記暗号化されたポイント情報の補充依頼

及びポイント使用情報を受け取った管理センタ211は、当該暗号を解読することでユーザ側200が要求しているポイント情報の補充量とポイント使用情報の内容を認識する。さらに、当該管理センタ211は、金融機関220に対して図6の(2)のように当該ポイント補充分の決済が可能かどうかの確認を行う。金融機関220にて、ユーザ側200の口座を調べることによって、決済可能であることが確認されると、当該金融機関220から図6の(3)のように決済OKの指示が管理センタ211に送られることになる。

【0037】また、このときの管理センタ211は、図6の(4)に示すように、コンテンツプロバイダ240に対して著作権者等の権利者に支払われることになるポイント使用数、すなわち金額を連絡する。

【0038】その後、管理センタ211では、ポイント補充情報の命令書を暗号化し、これをセキュリティIDと共にポイント補充指示情報として、図6の(5)に示すようにユーザ端末50に送る。このユーザ端末50からプレーヤ1に送られた上記ポイント補充指示情報は、当該プレーヤ1において復号化され、さらにセキュリティIDの確認後に、ポイント情報格納メモリ28へのポイント情報の補充と、ポイント使用情報格納メモリ29からの上記先に連絡した著作権情報等の権利者情報の削除とが行われる。

【0039】次に、デジタルコンテンツの鑑賞に伴ってユーザから徴収した課金代金、すなわちポイントの使用情報に応じてユーザの口座から引き落とされることになる代金の分配の手順では、先ず図7の(1)のようにユーザ側200に対して代金振り込み依頼が金融機関220からなされる。このとき、ユーザ側200の口座に十分な残高がある場合には、特に代金振り込み依頼はなされず、口座に十分な残高がない場合には、図7の(2)のようにユーザ側200から金融機関220に対して代金の振り込みがなされる。

【0040】金融機関220は、所定の手数料を差し引いて、図7の(3)のように、ユーザ側200から受け取った代金を管理センタ211に対して送金する。すなわち管理センタ211では、金融機関220から送金された上記代金から、コンテンツ加工料と金融手数料とシステム管理費等を徴収する。また、当該管理センタ211は、先に使用されたポイントに応じた著作権料を、図7の(4)のようにコンテンツプロバイダ240に対して支払うと共に、仮想店舗230に対しては図7の(5)のように店舗手数料を支払う。上記著作権料を受け取ったコンテンツプロバイダ240は著作権料を各著作権者に支払い、上記店舗手数料を受け取った仮想店舗230は仮想店舗毎の手数料を各仮想店舗に対して支払う。

【0041】このように、ユーザ側200から支払われた代金は、前記ポイント使用情報に基づいて、著作権料

と店舗手数料とコンテンツ加工手数料と決済手数料とシステム管理手数料とに分配され、上記著作権料はコンテンツプロバイダ240に、上記店舗手数料は上記仮想店舗230に、コンテンツ加工手数料はシステム管理会社210に、決済手数料はシステム管理会社と金融機関220に、システム管理手数料はシステム管理会社210に支払われる。

【0042】ここで、本実施の形態のシステム間でのデータ送受、すなわち管理センタ211とプレーヤ1との間のデータ送受の際には、データ通信の安全性を確保するために、通信するデータの暗号化及び復号化が行われる。本発明実施の形態では、暗号化及び復号化の方式として共通鍵暗号方式及び公開鍵暗号方式の何れにも対応可能となっている。

【0043】本発明の実施の形態では、上記デジタルコンテンツ、上記ポイント使用情報、ポイント情報、メッセージやセキュリティID、その他の各種情報の伝送の際の暗号方式としては、処理速度の点から共通鍵暗号方式を採用している。これら各種情報の暗号化及び復号化に使用する共通鍵は、それぞれ各情報に対応して異なるものである。前記図2のプレーヤ1では、管理センタ211から伝送されてくる暗号化された情報の復号化に使用する共通鍵が前記共通鍵保管メモリ22に保管され、この共通鍵保管メモリ22に保管している共通鍵を用いて、前記共通暗号復号回路24が、上記管理センタ211からの暗号化された情報の復号化を行う。

【0044】一方、上記各種情報の暗号化や復号化に使用する上記共通鍵の伝送の際の暗号方式としては、前記プレーヤ1の固有の鍵であるプレーヤ固有鍵が何れ的方式に対応しているかによって採用される暗号方式が変わるものである。すなわち、上記プレーヤ固有鍵が共通鍵暗号方式に対応している場合、上記共通鍵は当該プレーヤ固有鍵を用いて暗号化され、また当該暗号化された共通鍵は上記プレーヤ固有鍵を用いて復号化されることになる。これに対して、上記プレーヤ固有鍵が公開鍵暗号方式に対応している場合、上記共通鍵の暗号化には相手先の公開鍵が用いられ、暗号化された上記共通鍵の復号化にはそれぞれ復号化を行う側の秘密鍵が用いられる。

【0045】例えば上記プレーヤ1から管理センタ211に上記共通鍵（例えば後述するセッション鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記プレーヤ1では通信用鍵保管メモリ21が保管しているプレーヤ固有鍵を用いて上記共通鍵暗号復号回路24が上記共通鍵を暗号化し、管理センタ211では当該管理センタ211が保管しているプレーヤ固有鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。同じく、上記プレーヤ1から管理センタ211に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記プレーヤ1の通信用鍵保管メモリ

21が保管している管理センタ211の公開鍵にて上記公開鍵暗号復号回路20が上記共通鍵を暗号化し、管理センタ211では当該管理センタ211が保管している秘密鍵を用いて、上記暗号化されてる共通鍵の復号化を行う。

【0046】逆に、例えば上記管理センタ211からプレーヤ1に上記共通鍵（例えばコンテンツ鍵）が送られる場合において、上記プレーヤ固有鍵が共通鍵暗号方式に対応しているときには、上記管理センタ211が保管しているプレーヤ固有鍵にて上記共通鍵が暗号化され、プレーヤ1では上記通信用鍵保管メモリ21にて保管しているプレーヤ固有鍵を用いて、前記共通暗号復号回路24が上記暗号化されてる共通鍵の復号化を行う。同じく、上記管理センタ211からプレーヤ1に上記共通鍵が送られる場合において、例えば上記プレーヤ固有鍵が公開鍵暗号方式に対応しているときには、上記管理センタ211が保管しているプレーヤ1の公開鍵にて上記共通鍵が暗号化され、プレーヤ1では上記通信用鍵保管メモリ21にて保管しているプレーヤ固有鍵すなわち秘密鍵を用いて、前記公開暗号復号回路20が上記暗号化されてる共通鍵の復号化を行う。

【0047】上述したようなプレーヤ固有鍵自身の暗号方式は、当該プレーヤ固有鍵の配送（システム管理会社210からプレーヤ1への配送）が容易か否かによって決定されている。すなわち、コスト的には共通鍵暗号方式の方が有利であるので、プレーヤ固有鍵の配送が容易であれば共通鍵暗号方式を採用するが、当該プレーヤ固有鍵の配送が困難であるときにはコスト高であるが公開鍵暗号方式を採用する。プレーヤ固有鍵をハードウェアに実装する場合には共通鍵暗号方式を、ソフトウェアに実装する場合には公開鍵暗号方式を採用する。

【0048】以下、本発明の実施の形態では、プレーヤ固有鍵自身の暗号方式としてソフトウェアに実装する場合の互換性を考慮して、上記公開鍵暗号方式を採用する例を挙げて説明することにする。すなわち、上記管理センタ211とプレーヤ1との間で前記共通鍵の伝送が行われる場合において、上記プレーヤ1側で共通鍵（セッション鍵）が暗号化されるときには管理センタ211の公開鍵を用いて暗号化がなされ、管理センタ211では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。逆に、上記管理センタ211側で共通鍵（コンテンツ鍵）が暗号化されるときには、プレーヤの公開鍵にて暗号化がなされ、プレーヤ1では上記プレーヤ固有鍵（すなわち秘密鍵）を用いて上記暗号化されてる共通鍵の復号化を行う。

【0049】前述したような各手順と暗号方式を用いて運用されるシステムを構成する上記プレーヤ1とユーザ端末50と管理センタ211の実際の動作を、以下に順番に説明する。

【0050】先ず、上述したポイント補充すなわちボイ

10

20

30

40

50

ント購入時のプレーヤ1、ユーザ端末50、管理センタ10における処理の流れについて、図8から図11を用い、前記図2及び図3を参照しながら説明する。

【0051】図8には、ポイントを購入する際のプレーヤ1における処理の流れを示している。

【0052】この図8において、ステップST1では、ユーザ端末50すなわちパーソナルコンピュータに予めインストールされているポイント購入用のソフトウェアの立ち上げが行われ、この間のプレーヤ1のコントローラ16は、当該ポイント購入用のソフトウェアが立ち上

がるまで待っている。
【0053】上記ポイント購入用のソフトウェアが立ち上がると、ステップST2にて、プレーヤ1のコントローラ16は、上記ユーザ端末50に入力された情報を、当該ユーザ端末50から受信する。このときのユーザ端末50に入力される情報とは、上記ポイント購入用のソフトウェアに従って、上記ユーザ端末50を操作するユーザに対して当該ユーザ端末50から入力要求がなされるものであり、例えばパスワードや購入したいポイント情報数等の情報である。

【0054】これらユーザ端末50からの情報は、プレーヤ1のPC用インターフェース端子3及び当該プレーヤ1内に1チップ化された集積回路10の端子12を介して、コントローラ16に受信される。当該ユーザ端末50からの情報を受信したコントローラ16は、ステップST3にて、当該プレーヤ1の集積回路10内のパスワード格納メモリ14が格納するパスワードと、上記受信した情報中のパスワードとの比較を行い、上記受信パスワードが正しいかどうかの確認を行う。

【0055】上記パスワードが正しいと確認したコントローラ16は、ステップST4にて、ポイントを購入したい旨の情報（ポイント購入の主旨）と購入したいポイント情報数その他の情報を生成すると同時に、セキュリティID発生回路19からセキュリティIDを発生させ、次のステップST5にてこれらの情報を共通暗号復号回路24にて暗号化させる。コントローラ16は、次にステップST6にて、ユーザID格納メモリ23からユーザIDを読み出し、当該ユーザIDを上記暗号化した情報に付加し、さらに、ステップST7にて、当該ユーザIDを付加して作成したデータを上記端子12及びPC用インターフェース端子3を介してユーザ端末50に転送する。このユーザ端末50からは、上記作成データが管理センタ211に送られることになる。

【0056】このとき、上記作成データの暗号化には前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ16では、上記共通鍵として、例えば乱数発生手段であるセキュリティID発生回路19からセッション鍵を発生させる。また、この共通鍵（セッション鍵）は、上記作成データの伝送に先

だって、プレーヤ1から管理センタ211に対して送られることになる。ここで、当該共通鍵は前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ16では、上記共通鍵であるセッション鍵を公開暗号復号回路20に送ると同時に、通信用鍵保管メモリ21に予め保管されている管理センタ211の公開鍵を取り出して上記公開暗号復号回路20に送る。これにより当該公開暗号復号回路20では、上記管理センタ211の公開鍵を用いて上記共通鍵（セッション鍵）の暗号化が行われる。このようにして暗号化されたセッション鍵はユーザIDと共に、上記作成データの伝送に先だ

って管理センタ211に送られている。
【0057】なお、前述したように、ポイント情報の要求と共にポイント使用情報の転送も行う場合、コントローラ16は、ポイント使用情報格納メモリ29から前記権利者情報等を含むポイント使用情報を読み出し、これらも上記共通暗号復号回路26に送って暗号化させる。この暗号化したポイント使用情報は、上記作成データと共に伝送される。また、ポイント使用情報の転送と同時に、ポイント情報の残高をも同様にして転送することも可能である。

【0058】その後、コントローラ16は、ステップST8にて、ユーザ端末50を通して管理センタ211から送られてきた暗号化されているデータを受信する。この管理センタ211から送られてきたデータは、先に当該プレーヤ1から転送した上記購入したいポイント情報数に応じたポイント情報とセキュリティID等の情報が、上記セッション鍵と同じ共通鍵を用いて暗号化されたデータである。

【0059】コントローラ16は、上記管理センタ211からのデータを受信すると、ステップST9にて、当該データを上記共通暗号復号回路24に送ると共に、先に発生して共通鍵保管メモリ22に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路24に送る。当該共通暗号復号回路24では、上記共通鍵を用いて上記管理センタ211からの暗号化されたデータを復号化する。

【0060】次に、上記コントローラ16は、ステップST10にて、上記復号化されたデータのセキュリティIDを、上記セキュリティID発生回路19からのセキュリティIDとの比較によって確認し、その確認後、ステップST11にて、上記ポイント情報格納メモリ28に格納されていたポイント情報を、上記新たに送られてきたポイント情報にて修正する。

【0061】上記ポイント情報の修正等の処理が終了すると、コントローラ16は、ステップST12にて、処理完了のサインを生成し、上記共通鍵保管メモリ22から読み出した共通鍵と共に上記共通暗号復号回路24に送り、当該共通暗号復号回路24にて暗号化させる。その後、コントローラ16は、ステップST13にて当該

暗号化された処理完了のサインを、端子12及び3を介してユーザ端末50に転送し、管理センタ211に送る。

【0062】以上により、ポイント購入の際のプレーヤ1における処理の流れが終了する。

【0063】次に、上記ポイント購入時のユーザ端末50における処理の流れを、図9を用いて説明する。

【0064】この図9において、ユーザ端末50は、ステップST21にて、ポイント購入用のソフトウェアの立ち上げを行う。当該ポイント購入用ソフトウェアが立ち上がると、このユーザ端末50では、ステップST22にて、上記ポイント購入用のソフトウェアに従い当該ユーザ端末50を操作するユーザに対して上述したパスワードや購入したいポイント数等の情報の入力要求を行い、ユーザからこれらの情報が入力されると、当該入力された情報を前記図8のステップST2のように上記プレーヤ1に転送する。

【0065】次に、ユーザ端末50は、ステップST23にて、上記プレーヤ1から前記図8のステップST7のように作成されたデータを受信すると、ステップST24にて、当該プレーヤ1から転送されたデータを、予め登録されているアドレスすなわち管理センタ211へ転送する。

【0066】上記データの転送を行った後のユーザ端末50は、管理センタ211からの返送を待ち、管理センタ211からのデータ返送があると、ステップST25にて当該管理センタ211からのデータをそのままプレーヤ1に転送する。

【0067】当該ユーザ端末50は、ステップST26にて、上記プレーヤ1から前記図8のステップST13のように処理完了のサインを受信すると、当該ポイント購入等の処理が終了したことをユーザに知らせるために、ステップST27にて処理完了のサインをディスプレイに表示し、ユーザに確認させる。

【0068】その後、当該ユーザ端末50は、上記プレーヤ1から送られてきた処理完了のサインの暗号文を管理センタ211に転送する。

【0069】以上により、ポイント購入の際のユーザ端末50における処理の流れが終了する。

【0070】次に、ポイント購入時の管理センタ211における処理の流れを、図10を用いて説明する。

【0071】この図10において、管理センタ211は、ステップST31のように、コントロール機能部131にて全体が制御される管理機能ブロック130の通信機能部133によって、前記図8のステップST7及び図9のステップST24のようにユーザ端末50を介して転送されたプレーヤ1からの上記暗号化されたデータを受信する。このデータを受信すると、管理センタ211のユーザ管理機能ブロック110は、ステップST32のように、コントロール機能部111の制御の元

で、当該受信したデータに添付されたユーザIDに基づいて、データベース部112から共通鍵を入手すると共にセキュリティID発生機能部116からセキュリティIDを入手する。

【0072】なお、この時の共通鍵は、前記プレーヤ1から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、当該管理センタ211のユーザ管理機能ブロック110において、上記管理センタ211の公開鍵暗号方式の秘密鍵が取り出され、この秘密鍵と上記暗号化されているセッション鍵とが通信文暗号/復号機能部114に送られる。当該通信文暗号/復号機能部114では、上記管理センタ211の公開鍵を用いて上記暗号化されたセッション鍵の復号化が行われる。このようにして得られたセッション鍵（共通鍵）が上記データベース部112に格納されている。

【0073】上記データベース部112から上記ユーザIDに対応する共通鍵を入手すると共にセキュリティID発生機能部116からセキュリティIDを入手すると、ステップST33に示すように、管理センタ211のユーザ管理機能ブロック110の通信文暗号/復号機能部114において、上記共通鍵を用いて、上記プレーヤ1からの上記暗号化されたデータの復号化を行い、さらにコントロール機能部111において、当該復号化したデータ中のセキュリティIDと上記セキュリティID発生機能部116から読み出したセキュリティIDとの比較によって、アクセスしてきたユーザ側200（プレーヤ1）が正当な使用者であるかどうかの内容確認を行う。

【0074】上記アクセス元の正当性を確認した管理センタ211では、ステップST34のように、ユーザ管理機能ブロック110のポイント発生機能部113にて、上記ユーザ端末50から送られてきたデータの内容に応じたポイント情報の発行を行い、また、決済請求機能部117にて、ユーザの決済機関（金融機関220）への請求準備を行う。

【0075】さらに、管理センタ211は、ステップST35のように、例えばコントロール機能部111において、プレーヤ1からのポイント情報の残高とポイント使用情報に不正が無いことを確認し、後の処理のために情報のまとめを行う。すなわち、ポイント情報の残高と実際に使用したポイント情報の数とから不正な使用がないかどうかの確認とまとめを行う。なお、この確認とまとめは、必ず行わなければならないものではないが、望ましくは行った方が良い。

【0076】管理センタ211のユーザ管理機能ブロック110ではまた、上記ステップST35の処理の後、ステップST36のように、セキュリティID発生機能

部115において上記プレーヤ1（ユーザ）への新たなセキュリティIDを例えば乱数発生に基づいて算出し、さらに、例えばコントロール機能部110にて、上記セキュリティIDを上記ポイント情報と共に暗号化する。このときの暗号化も前記プレーヤ1から予め送られてきている前記セッション鍵（共通鍵）を用いて行う。

【0077】上記暗号化が終了すると、管理センタ211の管理機能ブロック130の通信機能部133では、コントロール機能部131の制御の元、上記暗号化したデータを前記図9のステップST25及び図8のステップST8のようにユーザ端末50を介してプレーヤ1に転送する。

【0078】その後、管理センタ211の通信機能部133において、ステップST38のように、前記図9のステップST28に示したユーザ端末50からの処理完了サインを受信して復号化すると、管理センタ211のユーザ管理機能ブロック110の決済請求機能部117では、ステップST39のように、当該処理完了サインに基づいて金融機関220に決済を請求する。この金融機関220に対する決済請求は、管理機能ブロック130の通信機能部132から行われる。

【0079】以上により、ポイント購入の際の管理センタ211における処理の流れが終了する。

【0080】上述した図8から図10の処理の流れにおけるプレーヤ1とユーザ端末50と管理センタ211との間の情報送受のシーケンスは、図11に示すように表すことができる。

【0081】すなわちこの図11において、入力情報転送T1では、前記図8のステップST2及び図9のステップST22のように、ユーザ端末50からプレーヤ1に対して、前記パスワードやポイント数等の入力情報が転送される。

【0082】作成データ転送T2では、前記図8のステップST7及び図9のステップST23のように、プレーヤ1からユーザ端末50に対して、前記プレーヤ1にて作成したデータが転送される。また、データ転送T3では、前記図9のステップST24及び図10のステップST31のように、ユーザ端末50から管理センタ211に対して、前記プレーヤ1が作成したデータが転送される。

【0083】データ転送T4では、前記図10のステップST37及び図9のステップST25のように、管理センタ211からユーザ端末50に対して、管理センタ211にて暗号化したデータが転送される。また、転送T5では、前記図9のステップST25及び図8のステップST8のように、管理センタ211からのデータをユーザ端末50がそのままプレーヤ1に転送される。

【0084】処理完了サイン転送T6では、前記図8のステップST13及び図9のステップST26のように、プレーヤ1からの処理完了サインがユーザ端末50

に転送される。さらに、処理完了サイン暗号文転送では、前記図9のステップST28及び図10のステップST38のように、プレーヤ1からの暗号化された処理完了サインが管理センタ211に転送される。

【0085】次に、上述したデジタルコンテンツの入手時のプレーヤ1、ユーザ端末50、管理センタ211における処理の流れについて、図2及び図3を参照しながら、図12から図15を用いて説明する。

【0086】図12には、デジタルコンテンツの入手時のプレーヤ1における処理の流れを示している。

【0087】この図12において、コントローラ16は、ステップST41のように、ユーザ端末50すなわちパーソナルコンピュータに予めインストールされているデジタルコンテンツ入手用のソフトウェアの立ち上げが行われるまで待っている。

【0088】上記デジタルコンテンツ入手用のソフトウェアが立ち上がると、コントローラ16は、ステップST42のように、ユーザ端末50を介して管理センタ211からデジタルコンテンツを含むデータを受信する。このときユーザ端末50から端子3及び12を介して受信するデータは、前述したようにコンテンツ鍵（コンテンツ毎に異なる共通鍵）で暗号化されたデジタルコンテンツと、当該デジタルコンテンツに対応するコンテンツIDとを少なくとも有してなる。したがって、この暗号化されたデジタルコンテンツを使用するには、コンテンツ鍵を管理センタ211から入手しなければならない。このコンテンツ鍵の入手の方法については後述する。

【0089】このユーザ端末50からのデータを受信したコントローラ16は、このデータすなわち暗号化されたデジタルコンテンツを、集積回路10の端子11を介し、記憶メディア用I/O端子4に接続されている記憶メディアに格納する。なお、この記憶メディアとしては、書き換え可能な光ディスクや半導体メモリ等の各種の記憶媒体が考えられるが、ランダムアクセス可能なものが望ましい。

【0090】以上により、デジタルコンテンツの入手時のプレーヤ1における処理の流れが終了する。

【0091】次に、デジタルコンテンツの入手時のユーザ端末50における処理の流れを、図13を用いて説明する。

【0092】この図13において、ユーザ端末50は、ステップST51にて、デジタルコンテンツ入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末50では、ステップST52にて、上記デジタルコンテンツ入手用のソフトウェアに従い、予め登録されているアドレスの管理センタ211にアクセスする。

【0093】このとき、当該管理センタ211は、前記仮想店舗230を用いて複数のデジタルコンテンツを

展示している。ユーザ端末50からは、ステップST53にて、この仮想店舗230に展示されている複数のデジタルコンテンツのなかから、ユーザの選択操作に応じた所望のデジタルコンテンツが指定される。すなわち、ユーザ端末50は、ステップST54のように、仮想店舗230に展示されたデジタルコンテンツの中の所望のデジタルコンテンツを指定するためのコンテンツの指定情報を管理センタ211に送信する。

【0094】ステップST55のように、上記コンテンツ指定情報に応じて管理センタ211から返送されたデータ、すなわち前記暗号化されたデジタルコンテンツ及びコンテンツIDからなるデータを受信すると、当該ユーザ端末50は、ステップST56のように、内部の例えばハードディスクやメモリ等の格納手段に上記データを一旦格納する。

【0095】その後、ユーザ端末50は、当該格納したデータ（暗号化されたデジタルコンテンツ及びコンテンツID）を、前記図12のステップST42のようにプレーヤ1に転送する。

【0096】以上により、デジタルコンテンツの入手時のユーザ端末50における処理の流れが終了する。

【0097】次に、デジタルコンテンツ入手時の管理センタ211における処理の流れを、図14を用いて説明する。

【0098】ここで、図3に示す管理センタ211は、前述した仮想店舗230に複数のコンテンツを展示させている。具体的には、管理センタ211のコンテンツ管理機能ブロック100において、前記仮想店舗230を生成しており、この仮想店舗230に上記複数のデジタルコンテンツの展示を行っている。

【0099】このように仮想店舗230にデジタルコンテンツを展示している状態で、図14のステップST61のように、前記図13のステップST54にてユーザ端末50からコンテンツ指定情報を受信する。

【0100】当該ユーザ端末50から上記コンテンツ指定情報を受信すると、コンテンツ管理機能ブロック100のコントロール機能部101は、このコンテンツ指定情報を管理機能ブロック130に送る。管理機能ブロック130のコントロール機能部131は、上記コントロール管理機能ブロック100から受け取ったコンテンツ指定情報を、権利者用の通信機能部134を通して、前記コンテンツプロバイダ240に転送する。これにより当該コンテンツプロバイダ240からは、上記コンテンツ指定情報にて要求されたデジタルコンテンツが転送されてくる。上記コンテンツプロバイダ240から入手したデジタルコンテンツは、管理機能ブロック130からコンテンツ管理機能ブロック100に送られ、このコンテンツ暗号・圧縮化機能部104に入力される。このとき、コントロール機能部101は、コンテンツ鍵・ID発生機能部103にて発生されてデータベース10

2に格納されているコンテンツ鍵を、上記コンテンツ暗号・圧縮化機能部104に送る。このコンテンツ暗号・圧縮化機能部104では、上記デジタルコンテンツに対して上記コンテンツ鍵を用いた暗号化を施し、さらに所定の圧縮処理を施す。コントロール機能部101は、上記暗号化及び圧縮処理されたデジタルコンテンツに対して、データベース102から取り出したコンテンツIDを付加し、管理機能ブロック130に送る。なお、デジタルコンテンツがオーディオ信号である場合の所定の圧縮処理としては、例えば近年製品化されているいわゆるMD（ミニディスク：商標）にて使用されている技術である、いわゆるATRAC（Adaptive Transform Acoustic Coding）のように、人間の聴覚特性を考慮してオーディオデータを高能率圧縮する処理を一例とした挙げることができる。

【0101】その後、図14のステップST62に示すように、管理機能ブロック130のコントロール部131は、ユーザ端末との通信機能部133を通して、上記暗号化及び圧縮処理されてコンテンツIDが付加されたデジタルコンテンツを、上記ユーザ端末50に送信する。

【0102】デジタルコンテンツ入手時の管理センタ211における処理の流れは以上である。

【0103】上述した図12から図14の処理の流れにおけるプレーヤ1とユーザ端末50と管理センタ211との間の情報送受のシーケンスは、図15に示すように表すことができる。

【0104】すなわちこの図15において、入力情報転送T11では、前記図13のステップST54のように、ユーザ端末50から管理センタ211に対して、前記コンテンツ指定情報が転送される。コンテンツ転送T12では、管理センタ211から、前記図14のステップST62のように、暗号化されたデジタルコンテンツとコンテンツIDがユーザ端末50に転送される。

【0105】コンテンツ転送T13では、前記図13のステップST57及び図12のステップST42のように、ユーザ端末50に一旦格納された上記暗号化されたデジタルコンテンツとコンテンツIDがプレーヤ1に転送される。

【0106】次に、上述したデジタルコンテンツを使用する際に必要となるコンテンツ鍵とその使用条件の入手時のプレーヤ1、ユーザ端末50、管理センタ211における処理の流れについて、図2及び図3を参照しながら、図16から図19を用いて説明する。

【0107】図16には、コンテンツ鍵及び使用条件の入手時のプレーヤ1における処理の流れを示している。

【0108】この図16のステップST71では、プレーヤ1のコントローラ16において、ユーザ端末50に予めインストールされているコンテンツ鍵及び使用条件入手用のソフトウェアの立ち上げが行われるまで待つて

いる。

【0109】上記ユーザ端末50の上記コンテンツ鍵及び使用条件入手用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末50に入力された情報が、ステップST72のように、前記PC用インターフェース端子3及び集積回路10の端子12を介して受信される。このときの上記ユーザ端末50から供給される入力情報は、鑑賞したいデジタルコンテンツの暗号化を解くのに必要なコンテンツ鍵を要求するための情報である。なお、この例では、上記コンテンツ鍵の要求情報として、このコンテンツ鍵を使用するデジタルコンテンツの指定情報を用いている。

【0110】このコンテンツ指定情報を上記ユーザ端末50から受信したコントローラ16は、ステップST73にて、当該コンテンツ指定情報にて指定されたデジタルコンテンツのIDと、セキュリティID発生回路19からのセキュリティIDとを作成し、この作成したデータを共通暗号復号回路24にて暗号化させる。また、コントローラ16は、当該作成したデータにユーザID格納メモリ23から読み出したユーザIDを付加し、上記端子12及びPC用インターフェース端子3を介してユーザ端末50に転送する。このユーザ端末50からは、上記作成データが管理センタ211に送られることになる。

【0111】このときの作成データの暗号化にも、前述したように共通鍵暗号方式が採用されているため、当該作成データの伝送に先立ち、共通鍵の生成が行われる。このため、上記コントローラ16では、上記共通鍵として、例えば乱数発生手段であるセキュリティID発生回路19からセッション鍵を発生させる。また、この共通鍵(セッション鍵)は、上記作成データの伝送に先だつて、プレーヤ1から管理センタ211に対して送られることになる。当該共通鍵は、前述のように公開鍵暗号方式にて暗号されるものであるため、上記コントローラ16では、上記共通鍵であるセッション鍵を公開暗号復号回路20に送ると同時に、通信用鍵保管メモリ21に予め保管されている管理センタ211の公開鍵を取り出して上記公開暗号復号回路20に送る。これにより当該公開暗号復号回路20では、上記管理センタ211の公開鍵を用いて上記共通鍵(セッション鍵)の暗号化が行われる。このようにして暗号化されたセッション鍵が、上記作成データの伝送に先だつて管理センタ211に送られている。

【0112】その後、コントローラ16は、ステップST75にて、後述するようにユーザ端末50を介して管理センタ211から送付されてきた暗号化されたデータを受信する。このときの管理センタ211から送られてきたデータは、後述するように上記コンテンツ鍵と使用条件とセキュリティID等が暗号化されたものである。

【0113】上記管理センタ211からの暗号化された

データを受信すると、プレーヤ1では、ステップST76のように、上記暗号化されたデータを復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ16は、上記復号化されたデータのセキュリティIDを、上記セキュリティID発生回路19からのセキュリティIDとの比較によって確認することによる正当性の評価を行う。

【0114】ここで、コンテンツ鍵については後述するように公開鍵暗号方式にて暗号化がなされ、使用条件及びセキュリティIDについては共通鍵暗号方式にて暗号化がなされている。したがって、当該暗号化されているコンテンツ鍵を復号化するには、公開鍵暗号方式の秘密鍵が必要であり、本実施の形態のプレーヤ1では前述したようにプレーヤ固有鍵を秘密鍵として使用することになっているので、当該プレーヤ固有鍵が通信用鍵保管メモリ21から取り出される。このプレーヤ固有鍵は、上記暗号化されたコンテンツ鍵と共に公開暗号復号回路20に送られる。この公開暗号復号回路20では、上記暗号化されているコンテンツ鍵を上記プレーヤ固有鍵を用いて復号化する。このように復号化されたコンテンツ鍵は、共通鍵保管メモリ22に保管される。一方、上記共通鍵暗号方式にて暗号化されている使用条件とセキュリティIDを復号化する場合には、これらのデータを上記共通暗号復号回路24に送ると共に、先に発生して共通鍵保管メモリ22に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路24に送る。当該共通暗号復号回路24では、上記共通鍵を用いて上記使用条件とセキュリティIDを復号化する。このように復号化された使用条件は、ポイント使用情報格納メモリ29に格納される。なお、ここで重要なのは、当該復号化されたコンテンツ鍵・使用条件は、当該プレーヤ1の外部、具体的には図2の集積回路10内に設けられたコントローラ16や共通鍵保管メモリ22、ポイント使用情報格納メモリ29から外部には取り出されないことである。

【0115】上記正当性の確認後、コントローラ16は、ステップST77のように、上記復号したコンテンツ鍵を上記コンテンツIDと共に上記共通鍵保管メモリ22に格納させる。

【0116】その後、コントローラ16は、ステップST78にて、上記コンテンツ鍵を入手した旨を示すメッセージを作成し、このメッセージを前述同様に共通鍵暗号復号回路24に送り、予め発生して共通鍵保管メモリ22に保管しておいた前記共通鍵を読み出して同じく共通暗号復号回路24に送る。当該共通暗号復号回路24では、上記共通鍵を用いてメッセージを暗号化する。

【0117】当該メッセージの暗号化が終了すると、コントローラ16は、ステップST79のように、この暗号化されたメッセージを端子12及び3を介してユーザ端末50に送信する。この暗号化されたメッセージは、その後、管理センタ211に転送させる。

10

20

30

40

50

【0118】以上より、コンテンツ鍵・使用条件入手時のプレーヤ1における処理の流れが終了する。

【0119】次に、コンテンツ鍵・使用条件入手時のユーザ端末50における処理の流れを、図17を用いて説明する。

【0120】この図17において、ユーザ端末50は、ステップST81にて、コンテンツ鍵・使用条件入手用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末50では、ステップST82にて、上記ソフトウェアに従い当該ユーザ端末50
10 を操作するユーザに対して、希望のコンテンツの指定入力要求を行い、ユーザからコンテンツの指定がなされると、その指定情報を生成する。ユーザ端末50は、上記ステップST83にて、上記コンテンツの指定情報をプレーヤ1に対して送信する。

【0121】次に、ユーザ端末50は、ステップST84にて、前記図16のステップST74のように上記プレーヤ1にて作成されて転送されたデータを受信すると、ステップST85にて、当該プレーヤ1から転送されたデータを、予めアドレスが登録されている管理セン
20 タ211へ転送する。

【0122】上記管理センタ211に対してデータの転送を行った後のユーザ端末50は、管理センタ211からの返送を待ち、ステップST86にて、管理センタ211から上記コンテンツIDで指定されたコンテンツ鍵・使用条件とセキュリティID等が暗号化されたデータの返送があると、ステップST87にて当該管理セン
タ211からのデータをそのままプレーヤ1に転送する。

【0123】上記プレーヤ1に対してデータの転送を行った後のユーザ端末50は、プレーヤ1からの返送を待
30 ち、ステップST88にて、プレーヤ1から前記図16のステップST79のように、上記コンテンツ鍵を入手した旨の暗号化されたメッセージの返送があると、ステップST89にて当該ユーザ端末50に接続されたディスプレイ装置に対して上記コンテンツ鍵入手が完了した旨の表示を行ってユーザに知らせる。

【0124】その後、上記プレーヤ1から返送された上記暗号化されたメッセージを、ステップST90にて、管理センタ211に送付する。

【0125】以上より、コンテンツ鍵・使用条件入手時のユーザ端末50における処理の流れが終了する。

【0126】次に、コンテンツ鍵・使用条件入手時の管理センタ211における処理の流れを、図18を用いて説明する。

【0127】この図18において、管理センタ211のユーザ端末との通信機能部133は、ステップST91にて、前記図16のステップST74及び図17のステップST85のようにユーザ端末50にてを介してプレーヤ1から送信されてきたコンテンツID、ユーザID、メッセージ、セキュリティIDの暗号化データを受
50

信する。この受信したデータは、ユーザ管理機能ブロック110に送られる。

【0128】当該ユーザ管理機能ブロック110のコントロール機能部111は、上記受信した暗号化データに付加されたユーザIDに基づいて、当該暗号化を解くための共通鍵をデータベース部112から取り出し、通信文暗号・復号機能部114ではこの共通鍵を用いて上記暗号化データを復号する。また、コントロール機能部111は、データベース部112から読み出したユーザIDとセキュリティID発生機能部116からのセキュリティIDとを用いて、上記受信して復号化したデータの正当性を確認する。

【0129】なお、この時の共通鍵は、前記プレーヤ1から予め送られてきている前記セッション鍵であり、このセッション鍵は前述のように公開鍵暗号方式にて暗号化されて送られてきたものである。したがって、この暗号化されているセッション鍵の復号時には、前述同様に当該管理センタ211において、上記管理センタ211の公開鍵暗号方式の秘密鍵が取り出され、当該通信文暗号/復号機能部114にて上記暗号化されているセッション鍵が秘密鍵を用いて復号化される。このようにして得られたセッション鍵（共通鍵）が上記データベース部112に格納されている。

【0130】上記受信したデータの正当性を確認すると、コントロール機能部111は、コンテンツ管理機能ブロック100に対して上記コンテンツIDにて指定されたコンテンツ鍵と使用条件を要求し、当該要求を受けたコンテンツ管理機能ブロック100のコントロール機能部101は、上記コンテンツIDにて指定されたコンテンツ鍵と使用条件とをデータベース部102から読み出してユーザ管理機能ブロック110に転送する。コントロール機能部111は、ステップST93に示すように、これらコンテンツ鍵と使用条件はセキュリティIDと共に通信文暗号/復号機能部114に送る。

【0131】ここで、コンテンツ鍵については前述した公開鍵暗号方式にて暗号化がなされ、使用条件及びセキュリティIDについては前述した共通鍵暗号方式にて暗号化がなされる。したがって、当該コンテンツ鍵を暗号化する時には、前記データベース部112からユーザ側200の公開鍵（プレーヤ1に対応して予め格納されている公開鍵）が上記ユーザIDに基づいて取り出されて通信文暗号/復号機能部114に送られる。当該通信文暗号/復号機能部114では、上記公開鍵を用いて上記コンテンツ鍵を暗号化する。一方、上記使用条件及びセキュリティIDを暗号化する時には、上記データベース部112から上記ユーザIDで指定された共通鍵（セッション鍵）が取り出されて通信文暗号/復号機能部114に送られる。このときの通信文暗号/復号機能部114では、上記使用条件及びセキュリティIDを上記共通鍵を用いて暗号化する。

【0132】上記暗号化されたコンテンツ鍵と使用条件及びセキュリティIDは、管理機能ブロック130に送られ、ステップST94のように、ユーザ端末との通信機能部133からユーザ端末50に送信される。このユーザ端末50に送信されたデータは、前記図17のステップST87及び図16のステップST75のようにユーザ端末50を介してプレーヤ1に送付されることになる。

【0133】その後、管理センタ211は、前記図16のステップST79及び図17のステップST90のようにプレーヤ1にて生成されてユーザ端末50を介して送信された暗号化メッセージの受信を待ち、ステップST95のように上記通信機能部133が上記プレーヤ1が生成した暗号化メッセージを受信すると、当該管理センタ211は、ステップST96のように、当該暗号化メッセージを共通鍵で復号化し、その復号メッセージから上記プレーヤ1がコンテンツ鍵と使用条件を入手したことを確認する。

【0134】以上により、コンテンツ鍵・使用条件入手時の管理センタ211における処理の流れが終了する。

【0135】上述した図16から図18の処理の流れにおけるプレーヤ1とユーザ端末50と管理センタ211との間の情報送受のシーケンスは、図19に示すように表すことができる。

【0136】すなわちこの図19において、コンテンツ指定情報転送T21では、前記図17のステップST83のように、ユーザ端末50からプレーヤ1に対して、前記コンテンツ指定情報が転送される。作成データ転送T22では、前記のステップST74のように、プレーヤ1にて作成されたデータがユーザ端末50に転送される。作成データ転送T23では、当該ユーザ端末50から上記プレーヤ1にて作成されたデータが管理センタ211に転送される。暗号化されたデータ送付T24では、前記図18のステップST94のように、管理センタ211にて暗号化されたデータがユーザ端末50に送付され、さらに、暗号化されたデータ送付T25では、当該暗号化されたデータがプレーヤ1に送付される。

【0137】メッセージ転送T26では、前記図16のステップST79のように、コンテンツ鍵入手完了を示すメッセージを暗号化したデータがプレーヤ1からユーザ端末50に転送され、さらに暗号化されたデータ送付T27では、上記プレーヤ1からの暗号化されたメッセージが、ユーザ端末50から管理センタ211に送付される。

【0138】次に、上述したようにしてポイント情報とデジタルコンテンツとコンテンツ鍵とを受け取ったプレーヤ1において、ユーザ端末50を用いてデジタルコンテンツを実際に鑑賞する際の処理の流れについて、図2を参照しながら図20を用いて説明する。

【0139】ここで、プレーヤ1の端子4には、前記デ

ジタルコンテンツが記憶された記憶メディアが接続されているとする。

【0140】この状態で、ステップST101のように、当該プレーヤ1に対して、ユーザ端末50から鑑賞を希望するデジタルコンテンツが指定される。このとき、当該指定は、例えばユーザ端末50をユーザが操作することによりなされる。

【0141】このとき、プレーヤ1のコントローラ16は、ステップST102のように、上記ユーザ端末50からのコンテンツ指定情報に応じて、上記記憶メディアに対するアクセスを行い、コンテンツのIDを読み取る。

【0142】上記コントローラ16は、ステップST103のように、上記記憶メディアから読み取ったコンテンツIDに基づき、前記共通鍵保管メモリ22に対してアクセスを行い、コンテンツ鍵が格納されているかどうかを確認すると共に、前記ポイント使用情報格納メモリ29に対してアクセスを行い、使用条件が格納されているかどうかを確認する。

【0143】ここで、上記共通鍵保管メモリ22やポイント使用情報格納メモリ29内に、上記コンテンツ鍵と使用条件が格納されていないことを確認したとき、コントローラ16は、ユーザ端末50に対して当該コンテンツ鍵等が存在しない旨の情報を送り、これによりユーザ端末50からは上記コンテンツ鍵等の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合は、前述したコンテンツ鍵入手用のフローチャートのようにしてコンテンツ鍵等を入手する。このように、新たにコンテンツ鍵等を入手した場合には、ステップST104にて前述したように、その暗号化されているコンテンツ鍵等を復号化する。

【0144】次に、コントローラ16は、ステップST105に示すように、上記復号化された使用条件を元に、ポイント情報格納メモリ28に格納されているポイント情報の残高が足りているかどうかを確認する。上記ポイント情報格納メモリ28に格納された上記ポイント情報の残高が足りないときには、コントローラ16からユーザ端末50に対して当該ポイント情報の残高が足りない旨の情報が送られ、これによりユーザ端末50は、上記ポイント情報の入手を促すメッセージを前記ディスプレイ装置に表示する。この場合、前述したようなポイント情報入手用のフローチャートのようにしてポイント情報を入手する。

【0145】ここで、実際にデジタルコンテンツの鑑賞を行うとき、コントローラ16は、ステップST106のように、当該鑑賞するデジタルコンテンツに応じて上記ポイント情報格納メモリ28からポイント情報数を減額し、さらに当該ポイント情報の使用状態に応じた新たなポイント使用情報を、ポイント使用情報格納メモリ29に格納する(ポイント使用情報の更新を行う)。

このようにポイント使用情報格納メモリ29に対して新たに格納されるポイント使用情報としては、上記鑑賞したデジタルコンテンツに対応する権利者情報（著作権者等）と減額されたポイント情報数の情報その他の情報などである。

【0146】その後、コントローラ16は、ステップST107のように、これらポイント情報の減額やポイント使用情報の新たな格納等の課金用処理が完了したことを確認すると、記憶メディアからデジタルコンテンツを読み出す。

【0147】この記憶メディアから読み出されたデジタルコンテンツは暗号化されているため、コントローラ16は、ステップST109のように、上記暗号化されたデジタルコンテンツを共通暗号復号回路24に転送する。

【0148】この共通暗号復号回路24では、ステップST110のように、コントローラ16からの指示に基づいて、先に復号化して共通鍵保管メモリ22に保管されているコンテンツ鍵を用いて、上記暗号化されているデジタルコンテンツの復号化を行う。

【0149】また、このデジタルコンテンツは前述したように所定の圧縮処理がなされているため、コントローラ16は、ステップST111のように、上記暗号が復号化された上記圧縮処理されているデジタルコンテンツを、上記共通暗号復号回路24から伸長回路26に転送させ、ここで上記所定の圧縮処理に対応する伸長処理を行わせる。

【0150】その後、当該伸長されたデジタルコンテンツは、ステップST112のように、D/A変換回路27にてアナログ信号に変換され、ステップST113のように、集積回路10の端子13と当該プレーヤ1のアナログ出力端子2とを介して外部（例えばユーザ端末50等）に出力される。

【0151】以上により、コンテンツ鑑賞時のプレーヤ1における処理の流れが終了し、ユーザはデジタルコンテンツの鑑賞が可能となる。

【0152】次に、上述したようなデジタルコンテンツの鑑賞に伴って前記プレーヤ1のポイント使用情報格納メディア29に新たに格納されたポイント使用情報を、管理センタ211に返却する際の、プレーヤ1、ユーザ端末50、管センタ310における処理の流れについて、図2と図3を参照しながら、図21から図24を用いて説明する。

【0153】図21には、ポイント使用情報返却時のプレーヤ1における処理の流れを示している。

【0154】この図21において、コントローラ16は、ステップST121に示すように、ユーザ端末50に予めインストールされているポイント使用情報返却用のソフトウェアの立ち上げが行われるまで待つ。

【0155】上記ユーザ端末50の上記ポイント使用情

報返却用のソフトウェアが立ち上がると、当該ソフトウェアに従ってユーザ端末50に入力された情報が、ステップST122のように、前記PC用インターフェース端子3及び集積回路10の端子12を介して受信される。このときの上記ユーザ端末50から供給される入力情報は、ユーザにより入力されるパスワード等である。

【0156】このコンテンツ指定情報を上記ユーザ端末50から受信したコントローラ16は、ステップST123にて、当該ユーザ端末50から供給されたパスワードと、パスワード格納メモリ14に格納されているパスワードとを比較して、当該パスワードが正しいかどうかの確認をする。

【0157】上記パスワードの確認において正しいパスワードであると確認されたとき、コントローラ16は、ステップST124のように、ポイント情報格納メモリ28に格納されているポイント情報の残高と、ポイント使用情報格納メモリ29に格納されているポイント使用情報とをそれぞれ読み出し、これら情報を暗号化する。

【0158】上記ポイント情報の残高とポイント使用情報の暗号化が終了すると、コントローラ16は、ステップST125のように、ユーザID格納メモリ23からユーザIDを読み出して上記暗号化したデータに添付する。

【0159】このユーザIDが添付されたデータは、ステップST126のように、コントローラ16から端子12及びPC用インターフェース端子3を介してユーザ端末50に転送される。このデータはその後管理センタ211に転送される。

【0160】なお、このときの暗号化にも前述したように共通鍵暗号方式が採用されている。すなわち、当該データの伝送に先立ち、前述同様に共通鍵の生成が行われ、この生成された共通鍵が前記公開鍵暗号方式にて暗号化（管理センタ211の公開鍵を用いた暗号化）され、ユーザIDと共に管理センタ211に送られている。

【0161】上述のようにしてユーザ端末50にデータを転送した後、コントローラ16は、上記管理センタ211から後述するデータがユーザ端末50を介して転送されてくるのを待つ。

【0162】ここで、ステップST127のように上記管理センタ211からのデータを受信すると、プレーヤ1では、ステップST127のように、共通鍵暗号方式を使用して暗号化されている受信データを、前述同様に共通鍵を用いて復号化すると共にそのデータの正当性の確認を行う。すなわち、コントローラ16は、上記復号化されたデータのセキュリティIDを、上記セキュリティID発生回路19からのセキュリティIDとの比較によって確認することによる正当性の評価を行う。

【0163】また、上記管理センタ211から転送されてくるデータには、上記共通鍵を用いて暗号化された処

理完了のメッセージも含まれている。したがって、上記セキュリティIDの確認が終了した後のコントローラ16は、上記暗号化された処理完了メッセージを共通暗号復号回路24に送り、ここで共通鍵を用いた復号化を行わせ、この復号化した処理完了メッセージを受け取ることで、上記管理センタ211での処理が完了したことを確認する。

【0164】以上により、ポイント使用情報返却時のプレーヤ1における処理の流れが終了する。

【0165】次に、ポイント使用情報返却時のユーザ端末50における処理の流れを、図22を用いて説明する。

【0166】この図22において、ユーザ端末50は、ステップST131にて、ポイント使用情報返却用のソフトウェアの立ち上げを行う。当該ソフトウェアが立ち上がると、このユーザ端末50では、ステップST132にて、上記ソフトウェアに従い当該ユーザ端末50を操作するユーザに対して、パスワード等の入力要求を行い、ユーザからパスワードの入力がなされると、そのパスワードをプレーヤ1に転送する。

【0167】次に、ユーザ端末50は、ステップST133にて、前記図21のステップST126のように上記プレーヤ1にて作成されて転送されたデータを受信すると、ステップST134にて、当該プレーヤ1から転送されたデータを、予めアドレスが登録されている管理センタ211へ転送する。

【0168】上記管理センタ211に対してデータの転送を行った後のユーザ端末50は、管理センタ211からの返送を待ち、ステップST135にて、管理センタ211からプレーヤ1に対して送られるデータを受信すると、当該データをそのままプレーヤ1に転送する。

【0169】上記プレーヤ1に対してデータの転送を行った後のユーザ端末50は、処理が完了した旨をユーザに知らしめるための表示をディスプレイ装置に行い、ユーザからの確認を受ける。

【0170】以上により、ポイント使用情報返却時のユーザ端末50における処理の流れが終了する。

【0171】次に、ポイント使用情報返却時の管理センタ211における処理の流れを、図23を用いて説明する。

【0172】管理センタ211のユーザ端末との通信機能部133において、ステップST141のように、前記図21のステップST126及び図22のステップST134によって前記ユーザ端末50を介してプレーヤ1から送信されてきたポイント使用情報等のデータを受信する。

【0173】このデータを受信すると、管理センタ211のユーザ管理機能ブロック110は、ステップST142のように、コントロール機能部111の制御の元で、当該受信したデータに添付されたユーザIDに基づ

いて、データベース部112から前述同様に予め受け取って格納している共通鍵を入手すると共にセキュリティIDを入手する。

【0174】上記データベース部112から上記ユーザIDに対応する共通鍵とセキュリティIDを入手すると、ステップST143に示すように、管理センタ211のユーザ管理機能ブロック110の通信文暗号/復号機能部114において、上記共通鍵を用いて、上記プレーヤ1からの上記暗号化されたポイント使用情報等のデータの復号化を行い、さらにコントロール機能部111において、当該復号化したデータ中のセキュリティIDと上記データベース部112から読み出したセキュリティIDとの比較によって、アクセスしてきたユーザ側200（プレーヤ1）が正当な使用者であるかどうかの内容確認を行う。

【0175】上記正当性と内容の確認後のデータは、使用情報管理機能ブロック120に転送される。この使用情報管理機能ブロック120のコントロール機能部121は、ステップST144に示すように、上記プレーヤ1から送られてきたポイント情報の残高とポイント使用情報とを用い、データベース部122に格納されている情報を用いて上記ユーザ側200の使用に不正がないかどうかの確認を行う。同時に、当該不正なきことを確認した場合には、使用情報演算機能部123においてポイント情報の残高とポイント使用情報をまとめる演算を行う。

【0176】その後、ステップST145に示すように、ユーザ管理機能ブロック110のコントロール機能部111は、セキュリティID発生機能部116を制御してセキュリティIDを算出させ、さらに確認メッセージ発生機能部115を制御して処理完了のメッセージを生成させる。これらセキュリティIDと処理完了メッセージは、ユーザ管理機能ブロック110の通信文暗号/復号機能部114にて前記共通鍵を用いて暗号化される。

【0177】上記暗号化されて生成されたデータは、ステップST146に示すように、ユーザ端末との通信機能部133からユーザ端末50に送られ、前記図22のステップST135と図21のステップST127のように当該ユーザ端末50からプレーヤ1に転送されることになる。

【0178】以上により、ポイント使用情報返却時の管理センタ211における処理の流れが終了する。

【0179】上述した図21から図23の処理の流れにおけるプレーヤ1とユーザ端末50と管理センタ211との間の情報送受のシーケンスは、図24に示すように表すことができる。

【0180】すなわちこの図24において、入力情報転送T31では、前記図22のステップST132のように、ユーザ端末50からプレーヤ1に対して、前記パス

ワード等の入力情報が転送される。作成データ転送T32では、前記図21のステップST126のように、プレーヤ1が作成したデータがユーザ端末50に転送される。作成データ転送T33では、前記図22のステップST134のように、上記プレーヤ1にて作成されたデータが上記ユーザ端末50から管理センタ211に転送される。データ転送T34では、前記図23のステップST146のように、管理センタ211にて作成されたデータが、ユーザ端末50に転送される。データ転送T35では、前記図21のステップST127のように、管理センタ211にて作成されたデータがユーザ端末50を介してプレーヤ1に転送される。

【0181】本実施の形態のシステムのプレーヤ1とユーザ端末50と管理センタ211の実際の動作は、上述したような流れとなる。

【0182】ここまでは、本実施の形態のシステムにおける全体の処理の流れを説明してきたが、これ以降は、本実施の形態のシステムの主要部の個々の動作を詳細に説明する。

【0183】まず、本発明実施の形態における暗号化及び圧縮と、伸長及び復号化の動作についての説明を行う。

【0184】上述した実施の形態のシステムのように、ネットワークを使ってデジタルコンテンツを配信する際には、そのデータ量を抑えるために圧縮/伸長技術を使用し、コピー防止或いは課金のために暗号化/圧縮技術が使われる。すなわち、配信側(上述の例では管理センタ211側)でデジタルコンテンツを圧縮し、さらに暗号化処理することが行われる。上述の例のように送信側(管理センタ211側)にて生成されたデジタルコンテンツ(暗号化/圧縮データ)をネットワークを使って配信するとき、受信側(上述の例ではプレーヤ1)では上記暗号化及び圧縮されたデジタルコンテンツを受信後に復号化し、さらに伸長してデジタルコンテンツを復元することが行われる。なお、上記暗号化と圧縮、復号化と伸長の処理の順番は入れ替わる場合もある。

【0185】上記デジタルコンテンツに著作権等が存在する場合、上記受信側は、上記デジタルコンテンツを上記復号化と伸長する際に、上記著作権者等の意思に従い、課金されることになる。この課金は、主として復号化の鍵すなわちコンテンツ鍵を購入することにより行われるが、このコンテンツ鍵を購入する方法には種々ある。

【0186】ここで、上述したように、デジタルコンテンツを圧縮して暗号化し、復号化して伸長するような処理手順に従った場合、例えば悪意を持ったユーザは上記復号化済みの圧縮データを比較的簡単に入手することができることになる。すなわちデジタルコンテンツの圧縮データは、一般に容量が大きく、したがって例えば

受信側の一般的なコンテンツ再生装置の内部メモリではなく、安価が外部メモリに蓄積される場合が多いため、この外部メモリから直接、或いは外部メモリとの接続部分で上記圧縮されたデジタルコンテンツを不正に取り出すことが容易だからである。

【0187】また、圧縮に対する伸長方式のアルゴリズムは公開されている場合が多く、また伸長方式のアルゴリズムには一般的な暗号の鍵のようにそれぞれ隠しておけば処理できないようなものも存在していない。しかも、上記復号化された圧縮デジタルコンテンツは、上記送信側から配信された暗号化と圧縮とがなされたデジタルコンテンツと比較して、データ量的に変わず、したがって、上記復号化された圧縮デジタルコンテンツを悪意を持って配信するのも容易である。すなわち、上記圧縮した後に暗号化されてデジタルコンテンツを配信する方式によると、誰でも容易に伸長できる圧縮デジタルコンテンツが、悪意を持ったユーザに容易に盗難され、このため著作権者等の意思の届かないところでさらに配信されたり、伸長されたりする危険性が大きい。

【0188】そこで、本発明の実施の形態では、このような状況に鑑み、ネットワークを使って配信するデジタルコンテンツの安全性を向上させることを可能にするため、上記図2のプレーヤ1において、以下の図25のフローチャートに示すような処理を行っている。

【0189】すなわち図2のプレーヤ1の共通暗号復号回路24における復号化処理と上記伸長回路26における伸長処理では、前記記憶メディアから読み出された暗号化と圧縮処理されたデジタルコンテンツのデータを、ステップST151のように、まず、復号化処理のアルゴリズムの処理単位Xビットと、伸長処理のアルゴリズム処理単位Yビットとの最小公倍数 $l\text{cm}(X, Y)$ の単位に分割する。

【0190】次に、上記最小公倍数 $l\text{cm}(X, Y)$ の単位に分割された上記暗号化と圧縮処理がなされているデジタルコンテンツのデータは、ステップST152に示すように、当該最小公倍数 $l\text{cm}(X, Y)$ の単位毎に、上記共通暗号復号回路24にて復号化処理が行われる。

【0191】当該復号化処理により得られた最小公倍数 $l\text{cm}(X, Y)$ の単位の圧縮されているデジタルコンテンツのデータは、ステップST154に示すように、当該単位分の全ての圧縮データに対して上記伸長回路26にて伸長処理が行われる。

【0192】その後、この最小公倍数 $l\text{cm}(X, Y)$ の単位毎の復号化及び伸長処理は、上記暗号化と圧縮処理されたデジタルコンテンツの全データについての処理が終了するまで続けられる。すなわち、ステップST155に示すように、最小公倍数 $l\text{cm}(X, Y)$ の単位毎の復号化及び伸長処理がデジタルコンテンツの全

データに対して完了したか否かの判断がなされ、完了していない時にはステップST152に戻り、完了したときに当該処理のフローチャートが終了する。

【0193】これにより全データの復号化及び伸長されたデジタルコンテンツが得られることになる。

【0194】なお、当該プレーヤ1における図25のフローチャートの処理でも、上記最小公倍数1cm(X, Y)単位の復号化データは存在することになるが、当該復号化データのデータ量は少ない。このため、比較的高価でも安全性の高い内部メモリに保存することができるように、したがって前述したような外部メモリに保存する場合のように盗まれる可能性は非常に低いものとなる。

【0195】また、本実施の形態における上記プレーヤ1では、上記安全性を確保するための内部メモリとして、図2のバッファメモリ25が上記共通暗号復号回路24と伸長回路26との間に設けられている。すなわちこのバッファメモリ25は、1チップの集積回路10内に設けられており、外部からアクセスされ難く、したがってデータが外部に取り出されることはない。

【0196】上述のフローチャートでは、最小公倍数1cm(X, Y)の単位分の全てのデータに対して復号化及び伸長処理を行うようにしており、このための具体的構成としては、例えば図26に示す構成のように、最初に復号化処理のアルゴリズムの処理単位Xビットにデジタルコンテンツのデータを分割し、このXビットのデータに復号化処理を施し、その後当該復号化処理されたXビットの圧縮されているデータを、伸長処理のアルゴリズム処理単位Yビット分まとめ、当該Yビットの圧縮データを伸長することで、上述のように最小公倍数1cm(X, Y)の単位での復号化及び伸長処理を実現するようにしている。

【0197】このことを実現するプレーヤ1の共通暗号復号回路24は、入力部30と暗号復号部31とからなり、上記伸長回路26は、伸長部32と出力部33とからなる。これら共通暗号復号回路24と伸長回路26の間に前記バッファメモリ25が設けられている。

【0198】ここで、より具体的な例として、上記デジタルコンテンツに対する暗号化処理が例えばDES(Data Encryption Standard)暗号を用いて行われているのであれば、当該暗号化処理とそれに対応する復号化処理は、64ビット単位で行われることになる。

【0199】また、圧縮されたデジタルコンテンツに対する伸長処理の場合、その圧縮率やサンプリング周波数によっても異なるが、現状では1K~2Kビット/チャンネル単位で処理される場合が多い。ここでは、便宜的に1.28Kビット毎に処理されると仮定する。

【0200】したがって、上記DES暗号化方式と上記1.28Kビット毎の圧縮伸長方式を用いたシステムの場合、上記最小公倍数1cmは1.28Kとなる。

【0201】このような条件のもと、図26の共通暗号復号回路24の入力部30には、前記暗号化されて圧縮されたデジタルコンテンツが入力される。当該入力部31では、上記暗号化されて圧縮されたデジタルコンテンツを、上記復号化処理のアルゴリズムの処理単位Xビット、すなわち64ビットずつのデータに分割して暗号復号部31に出力する。

【0202】この暗号復号部32では、上記Xビットすなわち64ビットのデータを、当該64ビット毎に復号化処理する。この64ビット毎の復号化により得られた64ビットの圧縮されているデータは、バッファメモリ25に送られる。

【0203】当該バッファメモリ25は、前記コントローラ16からの指示に従い、伸長処理のアルゴリズム処理単位Yビット、すなわち1.28Kビット分の圧縮データがたまった時点で、当該1.28Kビット分の圧縮データを一括して出力し、この圧縮データが上記伸長回路26の伸長部32に送られる。

【0204】上記伸長部26は、上記入力された1.28Kビット分の圧縮データを伸長して出力部33に出力する。

【0205】また、コントローラ16は、バッファメモリ25にたまったデータ量をモニタしながら、復号化部31の処理と伸長部32の処理をコントロールする。

【0206】なお、このケースであれば、復号化処理を20個(=1280/64)並列で処理すれば、より高速な処理システムになる。

【0207】その他、前記図2や図26のようなハードウェア構成ではなく、プログラマブルデバイスにて上述した処理を行う場合には、バッファメモリ25の状況に応じて、例えばコントローラ16が復号化プログラム或いは伸長プログラムに基づいて処理を行うことになる。

【0208】上述の説明では、圧縮した後に暗号化したデジタルコンテンツがプレーヤ1に供給され、プレーヤ1ではこの圧縮及び暗号化されたデジタルコンテンツを復号化した後に伸長する例を挙げたが、暗号化した後に圧縮されたデジタルコンテンツを伸長して復号化する場合であっても、上述同様の効果を得ることができる。

【0209】また、本発明は、圧縮/伸長並びに暗号化/復号化のアルゴリズムが限定されることはなく、いかなる方式に対しても有効である。

【0210】このように、本発明によれば、ネットワークを使って配信するデジタルコンテンツの安全性が向上する。

【0211】次に、前記セキュリティIDの発生動作についての説明を行う。

【0212】本実施の形態のように、ポイント情報を予め入手しておき、デジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、前述し

10

20

30

40

50

たように、ネットワーク上の管理センタ211は、ユーザ側200のユーザ端末50からのポイント情報の購入依頼の通信を受けた後に、金融機関220その他と任意の確認を行った後、そのポイント情報を暗号化して、ユーザ側200のプレーヤ1にネットワーク経由で送る。

【0213】本実施の形態のように、ポイント情報を予め入手しておき、デジタルコンテンツの鑑賞に応じて当該ポイント情報を減額するような方式の場合、管理センタ211とプレーヤ1（ユーザ端末50）との間で、ポイント情報の購入の度に、毎回同じようなデータのやり取りを行う（例えば暗号化された「3000円分のポイント情報の補充要求」及びそれに対応した「3000円分のポイント情報」といった情報のやり取りを行う）と、例えば悪意を持つ者による、金融機関220へのいわゆる「成り済まし」による金額補充が問題点となる。なお、ここに言う金融機関への「成り済まし」とは、上記悪意を持った者が本来のユーザ（本実施の形態ではユーザ側200）に成り済まして、不正にポイント情報を入手するようなことを言う。

【0214】すなわち、ポイント情報の購入の度に毎回同じようなデータのやり取りを行っている、例えば悪意を持った者が当該データを通信回線から盗み出して同じデータを生成し、管理センタ211に対して送り先を自分（悪意を持った者）にしてポイント情報の入手を依頼したような場合、当該悪意を持った者がポイント情報を入手できることになり、さらにこのポイント情報の購入代金の請求は本来のユーザ側200になされることになるという問題が発生するおそれがある。

【0215】そこで、こういった不正を防止するために、本発明実施の形態のシステムでは、予め受信側（プレーヤ1側）と配信側（管理センタ211側）の両者で連動している乱数発生機能により発生させられた乱数を安全性向上のために使用している。本実施の形態では、上記乱数として前記セキュリティIDを発生している。なお、両者間で乱数発生を連動させるには、例えばユーザの登録手続きなどの際に、例えばタイマ18を初期化するなどして、両者間の動作を同期させれば良い。

【0216】すなわち、この乱数（セキュリティID）を用いた場合の管理センタ211からプレーヤ1への例えばポイント情報入手時の動作は、以下のような流れとなる。

【0217】ポイント情報の購入時、管理センタ211からプレーヤ1に対して送られるデータは、前述したように例えばプレーヤ1から予め入手した共通鍵（セッション鍵）を用いて暗号化されたポイント情報と上記発生されたセキュリティIDからなるデータとなされる。

【0218】プレーヤ1のコントローラ16は、当該管理センタ211から受け取ったデータを前述したように共通暗号復号回路24に送り、ここで前記共通鍵を用いて復号化処理を行う。これにより、管理センタ211か

ら送られてきたポイント情報とセキュリティIDとが得られることになる。

【0219】その後、プレーヤ1のコントローラ16は、上記管理センタ211から送られてきたセキュリティIDと、自身のセキュリティID発生回路19にて発生したセキュリティIDとを比較する。この比較において、コントローラ16は、管理センタ211からのセキュリティIDと、上記自身が発生したセキュリティIDとが一致したときのみ、上記管理センタ211から送られてきたポイント情報を、前記ポイント情報格納メモリ28に格納する。

【0220】これにより、正当なユーザ側200のプレーヤ1のみがポイント情報を入手できることになる。言い換えれば、正当なユーザ側200のプレーヤ1と同じようなプレーヤを持っている悪意の者が、前記成り済ましによって不正にポイント情報を入手しようとしても、当該悪意の者が持っているプレーヤのセキュリティIDと上記管理センタ211から送られてきたセキュリティIDとは一致しないため、この悪意を持った者は前記成り済ましによる不正なポイント情報入手ができないことになる。

【0221】勿論、ユーザ側200のプレーヤ1で発生するセキュリティIDは、当該プレーヤ1の集積回路10内に設けられたセキュリティID発生回路19によって発生されるものであり、外部には取り出せないものであるため、悪意を持った者が当該セキュリティIDを盗むことはできない。

【0222】上記セキュリティIDとしての乱数を発生する構成には種々のものがあるが、その一例を図27に示す。この図27の構成は、前記図2のセキュリティID発生回路19の一具体例である。

【0223】この図27において、一方向関数発生部40は、いわゆる一方向性関数を発生する。なお、上記一方向性関数とは、比較的計算が簡単な関数で逆関数があるかに計算が困難なものである。この一方向関数は、予め秘密通信等で受け取って当該一方向関数発生部40に保存しておくことも可能である。なお、一方向関数発生部40は、前記図2の集積回路10内に設けられたタイマ18からの時間情報を入力関数として上記一方向関数を発生するようにすることも可能である。上記一方向関数は、乱数決定部43に送られる。

【0224】また、ユーザ定数発生部41は、ユーザ毎に定められた所定のユーザ定数を発生する。このユーザ定数は、予め秘密通信等で送付されて当該ユーザ定数発生部41に保存されるものである。なお、このユーザ定数は、例えば前記ユーザID格納メモリ23が格納するユーザIDを用いることもできる。

【0225】乱数データベース42は、乱数を格納するものであり、例えば99個の乱数を格納している。

【0226】通信回数記憶部44は、例えばコントロー

10

20

30

40

50

ラ16から送られてくる通信回数情報を記憶するものである。この通信回数情報とは、プレーヤ1と管理センタ211との間の通信回数を示す情報である。

【0227】これら一方向関数とユーザ定数と通信回数情報は、乱数決定部43に送られる。当該乱数決定部43は、例えば前記タイマ18からの時間情報に基づき、上記一方向関数とユーザ定数から、予め乱数データベース部42に記憶された範囲の乱数を発生させる（例えば99個）。

【0228】すなわち、この乱数決定部43では、上記通信回数情報が例えば1回目の通信であれば、99個目の乱数を上記乱数データベース部42から取り出し、また例えば通信回数情報がn回目の通信であれば100-n個目の乱数を上記乱数データベース42から取り出し、この取り出した乱数を前記セキュリティIDとして出力する。

【0229】このセキュリティID発生の構成は、プレーヤ1と管理センタ211とで同じものを有している。

【0230】なお、乱数データベース部42に格納している全ての乱数を使い終わったときには、上記乱数決定部42において100個～199個目の乱数を計算するか、或いは新たな乱数や1方向性関数を秘密通信するなどして、乱数データベース部42に再格納したり、一方向性関数発生部40に再構築する。

【0231】また、上述した説明では、乱数（セキュリティID）を発生させて通信毎の安全性を高めるようにしているが、本実施の形態では、前述のようにユーザ側200と管理センタ211側との間で通信を行う毎に、毎回異なる共通鍵（セッション鍵）をプログラマブルに発生させるようにもしているため、さらに安全性が高められている。

【0232】ここで、実際に送信される送信文（例えばメッセージ等）について上記乱数が挿入されると共にセッション鍵による暗号化がなされる様子と、受信文から乱数が取り出されて正当性の確認がなされる様子を図28と図29を用いて説明する。なお、これら図28、図29の例では、送信文に署名（デジタル署名）を付加するようにもしている。

【0233】この図28において、先ず、前記共通鍵を公開鍵暗号方式にて暗号化して送信する流れとして、通信用共通鍵発生工程P7では前記セッション鍵を通信用に用いる共通鍵として発生し、この共通鍵は公開鍵暗号化工程P8にて受信側の公開鍵で暗号化される。この暗号化された共通鍵は、受信側に送られる。

【0234】一方、送信文としてのメッセージを共通鍵暗号方式にて暗号化して送信する場合の流れとして、例えばメッセージ生成行程P1ではメッセージMが生成されると共に、乱数発生工程P5にて乱数（前記セキュリティID）が発生される。これらメッセージMと乱数は、共通鍵暗号化工程P6に送られる。この共通鍵暗号

化工程P6では、上記通信用共通鍵発生工程P7にて発生した共通鍵を用いて、上記メッセージMと乱数を暗号化する。

【0235】さらに、上記デジタル署名を付加する場合、上記メッセージMはハッシュ値計算工程P2に送られる。当該ハッシュ値計算工程P2では、上記メッセージMからいわゆるハッシュ値が計算される。なお、ハッシュ値とはハッシュ法にて求められるアドレス情報であり、ハッシュ法とはデータ（この場合はメッセージM）の内容の一部（キーワード）に所定の演算を施し、その結果をアドレスとして使用するものである。このメッセージから生成されたハッシュ値（M）はデジタル署名として、秘密鍵暗号化工程P4に送られる。この秘密鍵暗号化工程P4では、送信側の秘密鍵で上記デジタル署名を暗号化する。この暗号化されたデジタル署名は、共通鍵暗号化工程P6に送られる。これにより共通鍵暗号化工程P6では、上記通信用共通鍵発生工程P7にて発生した共通鍵を用いて、上記デジタル署名を暗号化する。

【0236】これらメッセージMとデジタル署名と乱数が受信側に送信される。

【0237】次に、図29を用いて、図28に対応する受信側での処理の流れを説明する。

【0238】この図29において、先ず、前記共通鍵を公開鍵暗号方式にて復号化する流れとして、秘密鍵復号化工程P11では、上記送信側から送信されてきた共通鍵を当該受信側の秘密鍵で復号化する。

【0239】一方、前記共通鍵暗号方式にて暗号化されたメッセージMを復号化する流れとして、共通鍵復号工程13では、上記送信されてきたメッセージMを上記秘密鍵復号化工程P11にて復号化した共通鍵を用いて復号化する。この復号化されたメッセージMは、他機能送信工程P20にて他の工程に送られることになる。

【0240】また、デジタル署名を復号する流れでは、上記共通鍵復号化工程P13にて復号化されたハッシュ値が、公開鍵復号化工程P14にて送信側の公開鍵を用いて復号化される。同時に、ハッシュ値計算工程P17では、上記メッセージMからハッシュ値を計算する。これら公開鍵復号化工程P14により復号化されたハッシュ値と上記ハッシュ値計算工程P17にて計算されたハッシュ値とは、比較工程P19にて比較され、改竄されていないことの確認が行われる。

【0241】さらに、送信された乱数については、上記共通鍵復号化工程P13にて復号化された乱数と、当該受信側の乱数発生工程P21にて発生された乱数とが、正当確認工程P22にて比較され、正当性の確認が行われる。

【0242】ところで、前述した図1に示した本実施の形態のシステムでは、ユーザ側200に対するシステム側として、システム管理会社210と仮想店舗230と

コンテンツプロバイダ240とが設けられている。なお、図1の金融機関220は、例えば外部の銀行等である。

【0243】上記システム管理会社210の管理センタ210は、仮想店舗230におけるデジタルコンテンツの展示や配信の管理、金融機関220との間でユーザ側200の課金情報や各種情報の収集、分配及びそれらの管理、コンテンツプロバイダ240からのデジタルコンテンツの暗号化、扱う情報のセキュリティ管理など、システム側の主要な作業のほぼ全てを行っている。

【0244】しかし、上述したようなネットワークを使ってデジタルコンテンツを配信するシステムにおいて、ユーザ側がシステム側からデジタルコンテンツを入手する際や、デジタルコンテンツの使用に伴う課金の際には、システム側に通信が集中することになり、ユーザ側に対して満足のいくレスポンスが得られなくなるおそれがある。

【0245】そこで、本発明の他の実施の形態では、システム管理会社210の機能、より具体的には管理センタ211の機能を、以下のように分割することで、上述したような通信の集中を防ぎ、通信のレスポンスを向上させることを可能にしている。

【0246】すなわち、本発明の他の実施の形態では、図30に示すように、ユーザ側200に対するシステム側の構成を、デジタルコンテンツを展示、配信する機能を有するコンテンツ展示配信機関310と、一定の地域のユーザの課金情報を管理する機能を有する課金情報管理機関320と、デジタルコンテンツを暗号化する等のデータ生成と上記コンテンツ展示配信機関310への生成データの配信と上記課金情報管理機関320からの情報収集と収益分配とシステム全体のセキュリティ管理その他を行う機能を有するシステム管理機関330とに分割し、各機関310、320、330がそれぞれ独立にユーザ側200と通信可能になされている。

【0247】この図30のような構成において、コンテンツ展示配信機関310は、世界中のネットワーク上に散らばって複数配置可能なものであり、ユーザ側200は通信費さえ支払えばどの地域のコンテンツ展示配信機関310へでもアクセスできる。例えばユーザ側200がデジタルコンテンツを入手したい場合には、ユーザ側200から上記コンテンツ展示配信機関310にアクセスして、デジタルコンテンツを入手する。このときのデジタルコンテンツは、システム管理機関330によって暗号化等されたデジタルコンテンツ、すなわちユーザ側200にネットワークを使って直接送信可能な状態になされたものである。

【0248】また、課金情報管理機関320は、課金情報を扱うため、余り多くのユーザを抱え込むことは安全性管理上好ましくなく、したがって、適度な数のユーザ毎に設置する。但し、あまり多く設置すると、悪意を持

った第三者からの攻撃ポイント（課金情報管理機関320）を増やすことになり、トレードオフになるので、最適化することが望ましい。例えばユーザ側200が課金に関する通信を行う場合には、ユーザ側200から上記課金情報管理機関320に対してアクセスする。

【0249】上記システム管理機関330は、ユーザのシステムへの加入や決済方法の登録、ユーザからの集金や前記権利者、コンテンツ展示配信機関310、課金情報管理機関320等の利益受益者への利益配付など、セキュリティ上重要な情報の管理をまとめて行うことで、セキュリティを向上させる。但し、当該システム管理機関330は世界に1箇所のみ設けるわけではなく、あるまとまった単位、例えば国などの単位で設置するのが望ましい。例えば、ユーザ側200がこのシステムへの加入や決済方法の登録などセキュリティ上重要な通信を行う場合には、ユーザ側200から上記システム管理機関330に対してアクセスして行う。当該ユーザからの集金と利益受益者への利益配付は上記課金情報管理機関320から情報を入手した当該システム管理機関330がまとめて行う。また、著作権者等が有するソースデータすなわちコンテンツは、当該システム管理機関330に供給され、ここで暗号化等がなされたデジタルコンテンツに変換され、上記コンテンツ展示配信機関310に配信される。

【0250】上述のように、システム側の機能を例えば3つの機関310、320、330に振り分け、ユーザ側200と各機関310、320、330との間で直接アクセス可能とすることにより、通信の集中を防ぎ、通信のレスポンスを向上させることが可能となる。また、コンテンツ展示配信機関310によれば、既存のいわゆるバーチャルモールのようなものにも対応でき、販売促進にも有効であり、ユーザにとって魅力のあるものになる。課金情報管理機関320を別に分けることにより、コンテンツの展示や販売機能と結託した不正防止に役立つ。また、管理するユーザを一定の数に抑えられるため、不正に対する管理機能もより効果的である。

【0251】以下に、上述した図30に示した本発明の他の実施の形態のシステムにおいて、ユーザのシステムへの加入、ポイント情報の購入や暗号化されたデジタルコンテンツの復号用のコンテンツ鍵等の入手時の情報の流れ、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れ、コンテンツの使用に伴う課金情報の流れについて説明する。

【0252】先ず、図31を用いて、ユーザのシステムへの加入時の流れの主要部を説明する。

【0253】ユーザのシステムへの加入登録の際には、システム管理機関330のユーザ加入サポート機能ブロック402による以下の手順の従って登録作業が行われる。

【0254】ユーザ側200すなわち前記プレーヤ1及

びユーザ端末50からは、先ず加入意思送付T41のように、システムへの加入の意思を示す情報が、システム管理機関330に対してネットワークを介して送付される。システム管理機関330の通信機能ブロック401に入力された上記加入意思の情報は、ユーザ加入サポート機能ブロック402に送られる。

【0255】当該ユーザ加入サポート機能ブロック402は、上記加入意思情報を受信すると、加入必要ファイル送付T42のように、加入に必要なファイルの情報を通信機能ブロック401を介してユーザ側200に送ら

れる。
【0256】ユーザ側200では、上記システム管理機関330から送られてきた加入必要ファイルに基づいて、所定のフォーマットに従った加入申請書の作成が行われる。当該作成された加入申請書は、加入申請書送付T43のように、システム管理機関330に送付される。

【0257】上記加入申請書を受け取ったユーザ加入サポート機能ブロック402は、クライアント機能送付T44のように、クライアントの機能を解説する情報を、ユーザ側200に送付する。

【0258】当該クライアント機能の情報を受け取ったユーザ側200からは、ユーザ情報送付T45のように、ユーザ側の情報、例えば前述したような口座番号やクレジット番号、名前や連絡先等のユーザ情報を、システム管理機関330に送付する。

【0259】当該ユーザ情報の送付を受けたユーザ加入サポート機能ブロック402は、登録手続き完了通知T46のように、加入の登録手続きが完了した旨の情報を、ユーザ側200に通知する。

【0260】また、このユーザ加入登録の手続き完了後、システム管理機関330のユーザ加入サポート機能ブロック402は、ユーザ情報送付T47のように、通信機能ブロック401を介して、課金情報管理機関320に対してユーザ情報を転送する。このユーザ情報を受け取った課金情報管理機関320は、当該ユーザ情報をデータベース機能ブロック367に保存する。

【0261】以上により、ユーザのシステムへの加入時の主な流れが終了する。なお、この図31に挙げられている他の構成についての説明は後述する。

【0262】次に、図32を用いて、ポイント情報の購入や暗号化されたデジタルコンテンツの復号用の鍵等の入手時の情報の流れの主要部を説明する。なお、上記ポイント情報の購入や暗号化されたデジタルコンテンツの復号用のコンテンツ鍵の情報は、コンテンツを使用するための情報であるので、以下の説明では、これらを簡略化して使用権情報と呼ぶことにする。

【0263】ユーザがシステムで使用する重要な情報（ここでは、コンテンツの使用権）を入手する際は、予めユーザ側200毎に担当割当がなされている課金情報

管理機関320に対し、ユーザ側200からアクセスがなされる。上記ユーザ側200から送られてくるコンテンツ使用権情報の入手要求のアクセスに対しては、課金情報管理機関320の使用権発行機能ブロック362が対応し、以下の手順に従って使用権の発行が行われる。

【0264】先ず、ユーザ側200からは、購入依頼書送付T51のように、使用権を購入したい旨の情報が課金情報管理機関320に対して送付される。使用権を購入したい旨の情報は、ユーザ側200によって所定のフォーマットに従った購入依頼書の情報である。このようにネットワークを介し、この課金情報管理機関320の通信機能ブロック361に入力された上記購入依頼書の情報は、使用権発行機能ブロック362に送られる。

【0265】当該使用権発行機能ブロック362では、上記購入依頼書の情報を受け取ると、データベース機能ブロック367に保存されたユーザ情報を元にして、新しい使用権の情報を生成し、新規使用権送付T52のように、当該使用権の情報をユーザ側200に対して送付する。

【0266】ユーザ側200は、上記新規使用権の情報の受取を確認すると、所定のフォーマットに従った受取確認書を作成し、受取確認書送付T53のように、課金情報管理機関320の使用権発行機能ブロック362に送付する。

【0267】以上により、使用権の購入時の主な流れが終了する。なお、この図32に挙げられている他の構成についての説明は後述する。

【0268】次に、図33を用いて、コンテンツとコンテンツ鑑賞用の情報（ここでは使用条件とコンテンツ

鍵）の流通の際の流れの主要部を説明する。
【0269】先ず、コンテンツ展示配信機関310のコンテンツ入手機能ブロック342は、コンテンツ請求書送付T62のように、システム管理機関330に対して、デジタルコンテンツを請求する。

【0270】当該コンテンツ請求書を受け取ったシステム管理機関330は、コンテンツ配布機能ブロック404において、要求されたコンテンツを流通できるように加工する。すなわち、このコンテンツ配布機能ブロック404では、ユーザ側200に送付可能な状態のデジタルコンテンツ（暗号化されたデジタルコンテンツ）を生成する。この加工されたデジタルコンテンツは、コンテンツ送付63のように、コンテンツ展示配信機関310に送られる。

【0271】当該コンテンツ展示配信機関310では、上記加工されたデジタルコンテンツを、コンテンツデータベース機能ブロック345に保存する。

【0272】また、システム管理機関330のコンテンツ配布機能ブロック404では、コンテンツ鑑賞用の情報として、コンテンツIDと使用条件と暗号化されたコンテンツを復号するためのコンテンツ鍵とを、コンテン

ツ鑑賞用情報送付T64のように、課金情報管理機関320に送付する。

【0273】課金情報管理機関320では、上記コンテンツ鑑賞用の情報を、コンテンツ鍵・使用条件受取機能ブロック363にて受理し、データベース機能ブロック367に保存する。

【0274】次に、ユーザ側200は、コンテンツ入手依頼T61のように、コンテンツ展示配信機関310に対してアクセスし、コンテンツを入手する。すなわち、コンテンツ展示配信機関310は、通信機能ブロック341を介して上記ユーザ側200からコンテンツの入手の要求がなされると、コンテンツデータベース機能ブロック354に保存している暗号化されたデジタルコンテンツを読み出し、当該読み出したデジタルコンテンツをユーザ側200の送付する。

【0275】その後、ユーザ側200は、コンテンツ鑑賞用情報請求T65にて課金情報管理機関320に対してアクセスし、コンテンツ鑑賞用情報送付T66のようにコンテンツ鑑賞用の情報を入手する。すなわち、課金情報管理機関320では、通信機能ブロック361を介して、上記ユーザ側200からコンテンツ鑑賞用の情報として使用条件とコンテンツ鍵の請求がなされると、コンテンツ鍵・使用条件発行機能ブロック364からコンテンツ鍵と使用条件とを発行し、これらを通信機能ブロック361を介してユーザ側200に送付する。

【0276】以上により、コンテンツとコンテンツ鑑賞用の情報の流通の際の流れが終了する。なお、この図33に挙げられている他の構成についての説明は後述する。

【0277】次に、図34を用いて、コンテンツが実際に鑑賞されたときの精算、すなわちコンテンツ使用料金の精算の流れの主要部を説明する。

【0278】先ず、ユーザ側200にてコンテンツの鑑賞が行われた後、当該ユーザ側200からは、精算書送付T71のように、例えば前述のようにしてポイント使用情報すなわちコンテンツの使用記録が課金情報管理機関320に対して送付される。このように通信機能ブロック361を介して上記ユーザ側200から上記コンテンツ使用記録の送付を受けると、課金情報管理機関320の精算手続き受付機能ブロック365にて当該コンテンツ使用記録を受け取り、これに対応する精算確認書を発行する。当該精算確認書は、精算確認書送付T73のように、同じく通信機能ブロック361を介してユーザ側200に送付される。これにより、ユーザ側200は精算が行われたことを知ることができる。

【0279】次に、課金情報管理機関320の精算手続き受付機能ブロック365は、使用権発行機能ブロック362から使用権発行情報を発行させる。この使用権発行情報は、上記ユーザ側200から送られてきたコンテンツ使用記録と共に、通信機能ブロック361を介し、

ユーザ決済・コンテンツ使用記録送付T74としてシステム管理機関330に送付される。

【0280】システム管理機関330は、集金及び分配機能ブロック405にて、各地に分散している課金情報管理機関320から送付されてきた情報をまとめ、集金額と集金先とお金の分配先を集計し、実際の金融機関を通して決済する。

【0281】以上により、コンテンツ使用料金の精算の流れが終了する。なお、この図34に挙げられている他の構成についての説明は後述する。

【0282】上述の図30から図34までの説明において、コンテンツ展示配信機関310、課金情報管理機関320、システム管理機関330とユーザ側200との間のデータ送受や、コンテンツ展示配信機関310、課金情報管理機関320とシステム管理機関330との間のデータ送受においても、前述同様にデータの暗号化と復号化が行われていることは言うまでもない。またこの暗号化と復号化においても、公開鍵暗号方式と共通鍵暗号方式の何れを用いても良いし、前述したようにコンテンツ鍵や共通鍵の暗号化方式としては公開鍵暗号方式を使用し、メッセージや各種の書類等の暗号化方式としては共通鍵暗号方式を使用することができる。また、これら暗号化と共に前記乱数を用いたセキュリティ向上の手法や、コンテンツを扱う際の暗号化と圧縮の処理単位の最小公倍数化を使用することも可能である。

【0283】次に、上述した各機関310、320、330の具体的な構成について簡単に説明する。

【0284】先ず、図35を用いてコンテンツ展示配信機関310の構成の説明を行う。

【0285】この図35において、当該コンテンツ展示配信機関310は、大別して、ユーザ側200とシステム管理機関330との間の通信機能を担当する通信機能ブロック341と、コンテンツの入手機能を担当するコンテンツ入手機能ブロック342と、コンテンツの展示機能を担当するコンテンツ展示機能ブロック343と、精算を担当する精算機能ブロック344と、コンテンツを保存するコンテンツデータベース機能ブロック345とからなる。

【0286】上記コンテンツ入手機能ブロック342は、システム管理機関330に対してコンテンツを請求するときの請求書の作成を担当するコンテンツ請求書作成機能部351と、システム管理機関330からコンテンツを受け取ったときの受領書の作成を担当するコンテンツ受領書作成機能部352と、これらあつかったコンテンツとコンテンツデータベース機能ブロック345に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部353とからなる。

【0287】上記コンテンツ展示機能ブロック343は、実際に仮想店舗にコンテンツを展示する機能を担当するコンテンツ展示機能部354と、これら展示してい

10

20

30

40

50

るコンテンツと上記コンテンツデータベース機能ブロック345に保存しているコンテンツとの対応を担当するコンテンツデータベース対応機能部355とからなる。

【0288】上記精算機能ブロック344は、領収書を発行する機能を担当する領収書発行機能部356と、金融機関220との間の対応を担当する金融機関対応機能部357とからなる。

【0289】次に、図36を用いて、課金情報管理機関320の構成の説明を行う。

【0290】この図36において、当該課金情報管理機関320は、大別して、ユーザ側200とシステム管理機関330との間の通信機能を担当する通信機能ブロック361と、使用権を発行する機能を担当する使用権発行機能ブロック362と、コンテンツ鍵と使用条件の受け取りを担当するコンテンツ鍵・使用条件受取機能ブロック363と、コンテンツ鍵と使用条件の発行を担当するコンテンツ鍵・使用条件発行機能ブロック364と、精算手続きの受け付け機能を担当する精算手続き受付機能ブロック365と、分配と受け取りの機能を担当する分配受取機能ブロック366と、データベース機能ブ

ック376とからなる。
 【0291】上記使用権発行機能ブロック362は、購入依頼書の確認機能を担当する購入依頼書確認機能部371と、クライアントすなわちユーザ側200の使用権の残高(ポイント情報の残高)や使用記録(ポイント使用情報)等のデータの確認を担当するポイントデータ確認機能部372と、使用権を発生する機能を担当する使用権発生機能部373と、使用権の送付書を作成する機能を担当する使用権送付書作成機能部374と、使用権と使用権送付書を実際に送付する機能を担当する送付機能部375と、使用権の受け取り書の確認を担当する使用権受取確認機能部376と、発行した使用権の情報を保存する機能を担当する使用権発行情報保存機能部377とからなる。

【0292】上記コンテンツ鍵・使用条件受取機能ブロック363は、コンテンツ鍵と使用条件の受取を担当する受取機能部378と、コンテンツ鍵と使用条件を保存する保存機能部379とからなる。

【0293】上記コンテンツ鍵・使用条件発行機能ブロック364は、コンテンツ鍵と使用条件の入手依頼を受信する機能を担当する受信機能部380と、コンテンツ鍵と使用条件をデータベース機能ブロック367から検索して探し出す機能を担当する検索機能部381と、コンテンツ鍵と使用条件を暗号化して送付する機能を担当する送信機能部382と、コンテンツ鍵と使用条件の受取書の確認機能を担当する確認機能部383とからなる。

【0294】上記精算手続き受付機能ブロック365は、暗号化されているコンテンツ使用記録(ポイント使用情報)を受信して復号化する機能を担当するコンテン

ツ使用記録受信機能部384と、コンテンツ使用記録の確認を担当するコンテンツ使用記録確認機能部385と、コンテンツ使用記録をデータベース機能ブロック367の保存する機能を担当するコンテンツ使用記録保存機能部386と、精算手続きの完了書を作成する機能を担当する完了書作成機能部387と、コンテンツ使用記録をまとめて編集する機能を担当するまとめ機能部389とからなる。

【0295】上記分配受取機能ブロック366は、集金を行う際の資料を請求する資料請求書の確認機能を担当する請求書確認機能部390と、システム管理機関330に対して提出するコンテンツ使用記録の報告書を作成する機能を担当する使用記録報告書作成機能部391と、システム管理機関330に対して提出する使用権発行情報の報告書を作成する機能を担当する使用権発行報告書作成機能部392と、報告書の受信確認書の確認機能を担当する確認書確認機能部393とからなる。

【0296】データベース機能ブロック367は、使用権のデータを保存する機能を担当する使用権データベース機能部394と、コンテンツ鍵と使用条件のデータを保存する機能を担当するコンテンツ鍵・使用権データベース機能部395と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部396と、ユーザに関する情報を保存するユーザ管理データベース機能部397とからなる。

【0297】次に、図37を用いて、システム管理機関330の構成の説明を行う。

【0298】この図37において、当該システム管理機関330は、大別して、ユーザ側200、コンテンツ展示配信機関310、及び課金情報管理機関320との間の通信機能を担当する通信機能ブロック401と、ユーザ加入の際のサポートを行うユーザ加入サポート機能ブロック402と、コンテンツの配布を担当するコンテンツ配布機能ブロック404と、データベース機能ブロック403と、集金と分配の機能を担当する集金及ぶ分配機能ブロック405とからなる。

【0299】上記ユーザ加入サポート機能ブロック402は、加入申請書の作成と送信を担当する加入申請書作成送信機能部411と、暗号化された共通鍵を受信して復号化する機能を担当する共通鍵受信機能部412と、ユーザ側200から送信されてきた加入申請書の確認機能を担当する加入申請書確認機能部413と、クライアントIDすなわちユーザIDを発生する機能を担当するID発生機能部414と、加入申請書をデータベース機能ブロック403に保存する機能を担当する加入申請書保存機能部415と、クライアント機能を生成するクライアント機能生成機能部416と、登録情報をデータベース機能ブロック403に保存する機能を担当する登録情報保存機能部417とからなる。

【0300】データベース機能ブロック403は、ユー

ザの情報を保存管理するユーザ管理データベース機能部418と、コンテンツを保存するコンテンツデータベース機能部419と、課金情報管理機関320の情報を保存管理する課金情報管理機関データベース機能部420と、コンテンツ展示配信機関310の情報を保存管理するコンテンツ展示配信機関データベース機能部421とからなる。

【0301】コンテンツ配信機能ブロック404は、コンテンツの請求書の確認機能を担当する請求書確認機能部422と、生コンテンツすなわち加工前のコンテンツ（ソースデータ）をデータベース機能ブロック403のコンテンツデータベース機能部419から検索する機能を担当するコンテンツ検索機能部423と、コンテンツIDを生成するコンテンツID生成機能部424と、コンテンツ鍵を生成するコンテンツ鍵生成機能部425と、コンテンツ使用条件を生成するコンテンツ使用条件生成機能部426と、生コンテンツすなわち加工前のコンテンツを圧縮するコンテンツ圧縮機能部427と、コンテンツの暗号化を行うコンテンツ加工機能部428と、コンテンツIDとコンテンツ鍵と使用条件とをデータベース機能ブロック403のコンテンツデータベース機能部419に保存する機能を担当する保存機能部429と、コンテンツを通信機能ブロック401を介して送付する機能を担当するコンテンツ送付機能部430と、コンテンツの受領書を確認する機能を担当するコンテンツ受領書確認機能部431と、コンテンツIDとコンテンツ鍵と使用条件を通信機能ブロック401を介して送付する機能を担当するID・鍵・使用条件送付機能部432と、コンテンツIDとコンテンツ鍵と使用条件の受領書を確認する機能を担当するID・鍵・使用条件受領書確認機能部433とからなる。

【0302】集金及び分配機能ブロック405は、集金に使用する資料の請求書を作成する資料請求書作成機能部434と、コンテンツ使用権を通信機能ブロック401を介して受信する機能を担当するコンテンツ使用権受信機能部435と、コンテンツ使用記録を通信機能ブロック401を介して受信する機能を担当するコンテンツ使用記録受信機能部436と、受信の確認書を作成する機能を担当する受信確認書作成機能部437と、ユーザへ請求する請求額の計算と請求書の作成を行う請求書の作成を行う計算・請求書作成機能部438と、使用により集金した使用金を権利者に分配する際の分配金の計算と納付書の作成を行う計算・納付書作成機能部439とからなる。

【0303】次に、当該他の実施の形態のシステムに対応するユーザ側200の構成を、図38を用いて説明する。なお、この図38は、前記プレーヤ1とユーザ端末50の各機能をまとめて表している。

【0304】この図38において、当該ユーザ側200の構成は、大別すると、システム管理機関330、コン

テンツ展示配信機関310、及び課金情報管理機関320との間の通信機能を担当する通信機能ブロック451と、コンテンツの入手を担当するコンテンツ入手機能ブロック452と、ポイント情報やコンテンツ鍵、使用条件等の使用権の購入を担当する使用権購入機能ブロック453と、コンテンツ鍵と使用条件の入手を担当するコンテンツ鍵・使用条件入手機能ブロック454と、精算手続きを担当する精算手続き機能ブロック455と、システムへの加入をサポートする機能を担当するユーザ加入サポート機能ブロック456と、コンテンツの鑑賞と課金の機能を担当するコンテンツ鑑賞課金機能ブロック457と、データベース機能ブロック458とからなる。

【0305】上記コンテンツ入手機能ブロック452は、実際にコンテンツを入手する機能を担当するコンテンツ入手機能部461と、コンテンツを記憶メディアに保存させる機能を担当するコンテンツ保存機能部462とからなる。

【0306】使用権購入機能ブロック453は、使用権の購入依頼書を作成する購入依頼書作成機能部463と、クライアント（ユーザ）の使用権の残高（ポイント残高）や使用記録（ポイント使用情報）等のデータのまとめを担当するまとめ機能部464と、使用権としての各情報をインストールする機能を担当する使用権インストール機能部465と、使用権受取書を作成する使用権受取書作成機能部467とからなる。

【0307】コンテンツ鍵・使用条件入手機能ブロック454は、コンテンツ鍵と使用条件の入手依頼書を作成する入手依頼書作成機能部468と、コンテンツ鍵と使用条件の受信を担当する受信機能部469と、コンテンツ鍵と使用条件の受取書を作成する受取書作成機能部470とからなる。

【0308】精算手続き機能ブロック455は、コンテンツ使用記録（ポイント使用情報）のまとめを行うまとめ機能部471と、精算手続きの完了書の受信を担当する完了書受信機能部472とからなる。

【0309】上記ユーザ加入サポート機能ブロック456は、加入申請書の作成を担当する加入申請書作成機能部473と、クライアント機能のインストールすなわちユーザのプレーヤ1の初期化を担当するクライアント機能インストール機能部474、登録情報を作成する機能を担当する登録情報作成機能部475とからなる。

【0310】コンテンツ鑑賞課金機能ブロック457は、記憶メディアに保存されたコンテンツの検索を担当するコンテンツ検索機能部476と、使用権の確認を担当する使用権確認機能部477と、例えばコンテンツの選択を行うときに簡易的にコンテンツを再生する簡易コンテンツ鑑賞機能部478と、課金情報（ポイント情報）の管理を行う課金機能部479と、暗号化されているコンテンツを復号化するコンテンツ復号機能部480

と、圧縮されているコンテンツを伸長するコンテンツ伸長機能部481と、例えば記憶メディアに保存されているコンテンツの内容を認識可能にするためのコンテンツビューア機能部482とからなる。

【0311】データベース機能ブロック458は、使用権のデータを保存する使用権データベース機能部483と、コンテンツ鍵と使用条件を保存するコンテンツ鍵・使用条件データベース機能部484と、コンテンツ使用記録を保存するコンテンツ使用記録データベース機能部485と、ユーザ情報を保存するユーザ情報データベース機能部486とからなる。

【0312】次に、上述したような各実施の形態のプレーヤ1とユーザ端末50の具体的な使用形態について、図39と図40を用いて説明する。

【0313】図39に示すように、プレーヤ1は、前記アナログ出力端子2とPC用インターフェース端子3と記憶メディア用I/O端子4がプレーヤ1の筐体外に突き出た状態で配置されており、上記記憶メディア用I/O端子4には、記憶メディア61が接続されるようになっている。また、これらプレーヤ1と記憶メディア61は、例えばケース60内に収納可能に形成されており、このケース60の例えば一端側に上記プレーヤ1のアナログ出力端子2とPC用インターフェース端子3が配置されるようになされている。

【0314】このプレーヤ1及び記憶メディア61が収納されたケース60は、上記プレーヤ1のアナログ出力端子2とPC用インターフェース端子3が配置される側から、上記ユーザ端末50としてのパーソナルコンピュータ50の入出力ポート53に挿入接続可能なように形成されている。

【0315】当該パーソナルコンピュータ50は、コンピュータ本体に、ディスプレイ装置52とキーボード54とマウス55とを備えた一般的な構成を有するものであるが、上記入出力ポート53内には上記プレーヤ1のアナログ出力端子2及びPC用インターフェース端子3と対応したインターフェースが形成されている。したがって、上記プレーヤ1及び記憶メディア61が収納されたケース60を上記パーソナルコンピュータ50の入出力ポート53に挿入するだけで、上記プレーヤ1のアナログ出力端子2とPC用インターフェース端子3が上記パーソナルコンピュータ50と接続されるようになる。

【0316】上記図39の例では、パーソナルコンピュータ50の入出力ポート53内に、上記プレーヤ1のアナログ出力端子2及びPC用インターフェース端子3と対応したインターフェースを形成するようにしているが、例えば図40に示すように、パーソナルコンピュータ50の汎用入出力ポートのインターフェースに対応できるアダプタ62を、上記プレーヤ1のアナログ出力端子2及びPC用インターフェース端子3の間に配置することも可能である。

【0317】以上述べてきたことから、本発明の実施の形態のシステムにおいては、デジタルコンテンツはシステムの共通鍵であるコンテンツ鍵にて暗号化されているので、本実施の形態のシステムに登録したユーザ（プレーヤ1）であれば、この暗号化されたコンテンツを自由にコピーでき、コンテンツ鍵を入手しさえすればこのコンテンツの鑑賞も可能である。したがって、このコンテンツ（暗号化されたコンテンツの）記憶メディアへのインストールも簡単に行える。一方、本実施の形態システムに準拠していない端末装置では、暗号化されたデジタルコンテンツを復号できないので、コンテンツの著作権や当該コンテンツの権利者の権利は保護される。

【0318】また、本発明の実施の形態システムによれば、ポイント情報をプリペイド方式（料金前払い方式）により補充することにし、コンテンツ鑑賞時にポイント情報が減額されるようにするとともに、そのポイントの使用情報を収集するようにしているので、使用済みのポイントに関する権利をもつ権利者（著作権者等）及びコンテンツ販売店舗等は、鑑賞代金の回収が可能である。

【0319】さらに、ポイント情報やポイント使用情報のデータのやりとりの際には、前述したように暗号化が施されているので、セキュリティ性が向上している。例えば全く前回のデータと同じものを偽造して課金用のポイント情報を盗もうとしても、前述したように、システム側とプレーヤ側とで連動した乱数（セキュリティID）を使用し、両者が一致していることを確認してから取引を行うものとしているので、安全である。

【0320】またさらに、プレーヤの主要構成要素は1チップ化されており、鍵情報や復号化されたデジタルコンテンツを外に取り出すことが困難となっている。このプレーヤ1は、当該プレーヤ1の破壊によるデータ横取りを防ぐためにプレーヤ1自体にタンパーレジスタンス機能を備えている。

【0321】上述したように、本発明の実施の形態によれば、セキュリティ上強度の高いデジタルコンテンツ配信システムが構築されている。

【0322】なお、上述のデジタルコンテンツとしては、デジタルオーディオデータの他に、デジタルビデオデータ等の各種のものを挙げることができる。上記デジタルビデオデータとして動画データ（オーディオデータも含む）を使用した場合、前記圧縮の手法としては、例えばMPEG（Moving Picture Image Coding Experts Group）等の圧縮手法を使用できる。なお、上記MPEGは、ISO（国際標準化機構）とIEC（国際電気標準会議）のJTC（Joint Technical Committee）1のSC（Sub Committee）29のWG（Working Group）11においてまとめられた動画像符号化方式の通称であり、MPEG1、MPEG2、MPEG4等がある。

【0323】さらに、上記暗号化の手法としては、前述

したように、例えばいわゆるDES (Data Encryption Standard) と呼ばれている暗号化手法を使用することができる。なお、DESとは、米国のNIST (National Institute of Standards and Technology) が1976年に発表した標準暗号方式 (暗号アルゴリズム) である。具体的には、64ビットのデータブロック毎にデータ変換を行うものであり、関数を使った変換を16回繰り返す。上記デジタルコンテンツやポイント情報等は、当該DESを用い、いわゆる共通鍵方式にて暗号化されている。なお、上記共通鍵方式とは、暗号化するための鍵データ (暗号鍵データ) と復号化するための鍵 (復号鍵データ) が同一となる方式である。

【0324】また、前記図1のプレーヤ1の共通鍵保管メモリ22や通信用鍵保管メモリ21、ポイント使用情報格納メモリ29、ポイント情報格納メモリ28等には、例えばいわゆるEEPROM (電氣的に消去可能なROM) を使用できる。

【0325】他に記憶メディアとしては、例えばハードディスクやフロッピディスク、光磁気ディスク、相変化型光ディスク等の記録媒体、或いは半導体メモリ (ICカード等) の記憶メディアを使用できる。

【0326】その他、上述の実施の形態では、コンテンツの選択や仮想店舗230に展示されたコンテンツの内容確認等の際には、ユーザ端末50のキーボード54やマウス55、ディスプレイ装置52を使用して選択、確認等を行っていたが、これらキーボードやマウス、ディスプレイ装置に機能を簡略化して、プレーヤ1に持たせることも可能である。すなわち、図2のように、入力キー部6や表示部7をプレーヤ1に設けることも可能である。

【0327】

【発明の効果】以上の説明で明らかなように、本発明によれば、通信相手側との間でデータ送受信を行う毎に乱数を発生し、データ送信時には送信データに乱数を付加し、データ受信側では受信データに付加された乱数と自己が発生した乱数とを比較して一致したときのみ受信データを正当なものとして扱うことにより、例えば単純な金額補充データの通信の際のいわゆる「成り済まし」を防ぐことが可能になった。

【図面の簡単な説明】

【図1】本発明の実施の形態のデジタルコンテンツ配布システムの全体構成を示すシステム構成図である。

【図2】本発明の実施の形態のシステムに対応するプレーヤの具体的な構成を示すブロック回路図である。

【図3】本発明の実施の形態のシステムに対応する管理センタの具体的な構成を示すブロック回路図である。

【図4】本実施の形態のシステムにおいてプレーヤの購入時の手順の説明に用いる図である。

【図5】本実施の形態のシステムにおいてデジタルコンテンツの検索からプレーヤ用の記憶メディアへのディ

ジタルコンテンツのインストールまでの手順の説明に用いる図である。

【図6】実施の形態のシステムにおいて課金用のポイント情報の購入と当該デジタルコンテンツを使用した場合の精算の手順の説明に用いる図である。

【図7】実施の形態のシステムにおいて課金代金の分配の手順の説明に用いる図である。

【図8】実施の形態のシステムにおいてポイント購入時のプレーヤにおける処理の流れを示すフローチャートである。

【図9】実施の形態のシステムにおいてポイント購入時のユーザ端末における処理の流れを示すフローチャートである。

【図10】実施の形態のシステムにおいてポイント購入時の管理センタにおける処理の流れを示すフローチャートである。

【図11】実施の形態のシステムにおいてポイント購入時の情報送受のシーケンスを示す図である。

【図12】実施の形態のシステムにおいてデジタルコンテンツの入手時のプレーヤにおける処理の流れを示すフローチャートである。

【図13】実施の形態のシステムにおいてデジタルコンテンツの入手時のユーザ端末における処理の流れを示すフローチャートである。

【図14】実施の形態のシステムにおいてデジタルコンテンツの入手時の管理センタにおける処理の流れを示すフローチャートである。

【図15】実施の形態のシステムにおいてデジタルコンテンツの入手時の情報送受のシーケンスを示す図である。

【図16】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のプレーヤにおける処理の流れを示すフローチャートである。

【図17】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時のユーザ端末における処理の流れを示すフローチャートである。

【図18】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の管理センタにおける処理の流れを示すフローチャートである。

【図19】実施の形態のシステムにおいてコンテンツ鍵及び使用条件の入手時の情報送受のシーケンスを示す図である。

【図20】実施の形態のシステムにおいてプレーヤとユーザ端末を用いてデジタルコンテンツを実際に鑑賞する際の処理の流れを示すフローチャートである。

【図21】実施の形態のシステムにおいてポイント使用情報返却時のプレーヤにおける処理の流れを示すフローチャートである。

【図22】実施の形態のシステムにおいてポイント使用情報返却時のユーザ端末における処理の流れを示すフロ

ーチャートである。

【図23】実施の形態のシステムにおいてポイント使用
情報返却時の管理センタにおける処理の流れを示すフ
ローチャートである。

【図24】実施の形態のシステムにおいてポイント使用
情報返却時の情報送受のシーケンスを示す図である。

【図25】暗号化と圧縮の処理単位の最小公倍数にて復
号化と伸長を行う際の処理の流れを示すフローチャート
である。

【図26】暗号化と圧縮の処理単位の最小公倍数の単位
毎の復号化及び伸長処理を行う構成を示すブロック回路
図である。

【図27】セキュリティIDとしての乱数を発生する具
体的構成を示すブロック回路図である。

【図28】共通鍵を公開鍵暗号方式にて暗号化して送信
する際に乱数が挿入される様子を説明するための図であ
る。

【図29】受信文から乱数が取り出されて正当性の確認
がなされる様子を説明するための図である。

【図30】システム側の機能を分割したときの各機関の
説明に用いる図である。

【図31】システム側の機能を分割した実施の形態にお
いて、ユーザのシステムへの加入時の流れの主要部を説
明するための図である。

【図32】システム側の機能を分割した実施の形態にお
いて、ポイント情報の購入や暗号化されたデジタルコン
テンツの復号用の鍵等の入手時の情報の流れの主要部
を説明するための図である。

【図33】システム側の機能を分割した実施の形態にお
いて、コンテンツとコンテンツ鑑賞用の情報の流通の際
の流れの主要部を説明するための図である。

【図34】システム側の機能を分割した実施の形態にお*

＊いて、コンテンツが実際に鑑賞されたときの精算の流れ
の主要部を説明するための図である。

【図35】システム側の機能を分割した実施の形態にお
いて、コンテンツ展示配信機関の構成を示すブロック図
である。

【図36】システム側の機能を分割した実施の形態にお
いて、課金情報管理機関の構成を示すブロック図であ
る。

【図37】システム側の機能を分割した実施の形態にお
いて、システム管理機関の構成を示すブロック図であ
る。

【図38】システム側の機能を分割した実施の形態にお
いて、ユーザ側の構成を示すブロック図である。

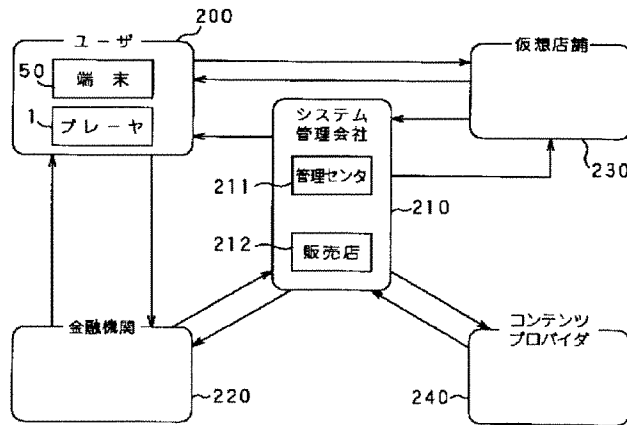
【図39】プレーヤとユーザ端末の具体的な使用形態の
一例の説明に用いる図である。

【図40】プレーヤとユーザ端末の具体的な使用形態の
他の例の説明に用いる図である。

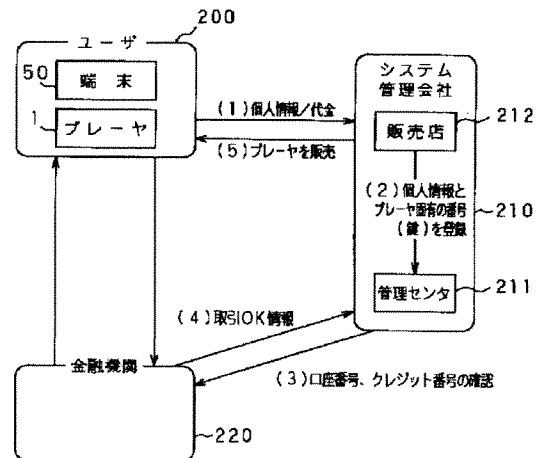
【符号の説明】

- 1 プレーヤ、 2 アナログ出力端子、 3 PC用
インターフェース端子、 4 記憶メディア用I/O端
子、 16 コントローラ、 19 セキュリティID
発生回路、 20 公開暗号復号回路、 21 通信用
鍵保管メモリ、 22 共通鍵保管メモリ、 23 ユー
ザID格納メモリ、 24 共通暗号復号回路、 25
バッファメモリ、 26 伸長回路、 27 D/A
変換回路、 50 ユーザ端末、 100 コンテンツ
管理機能ブロック、 110 ユーザ管理機能ブロック、
120 使用情報管理機能ブロック、 130 管理
機能ブロック、 200 ユーザ側、 210 システ
ム管理会社、 211 管理センタ、 220 金融機
関、 230 仮想店舗、 240 コンテンツプロバ
イダ

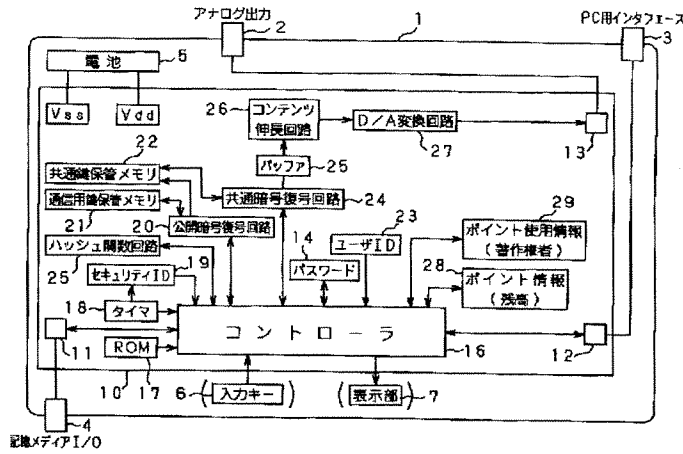
【図1】



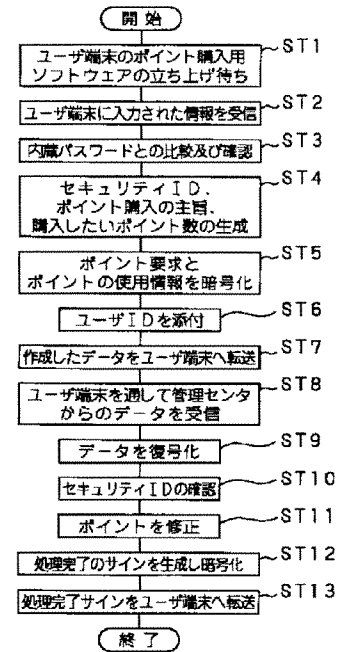
【図4】



【図2】

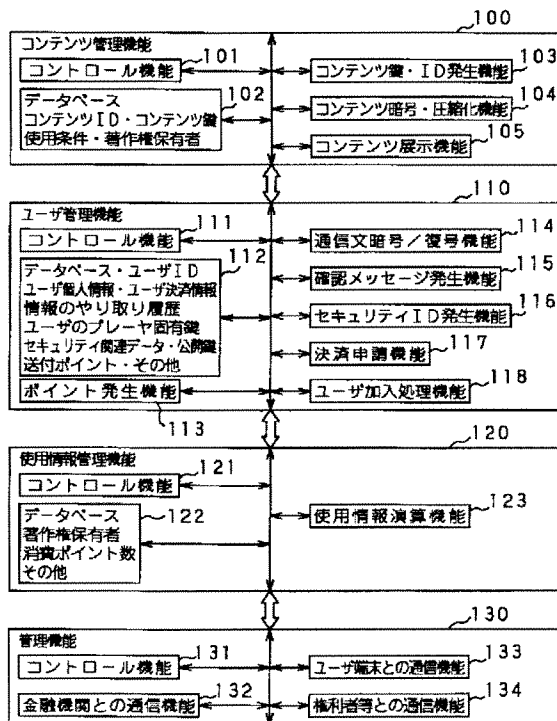


【図8】

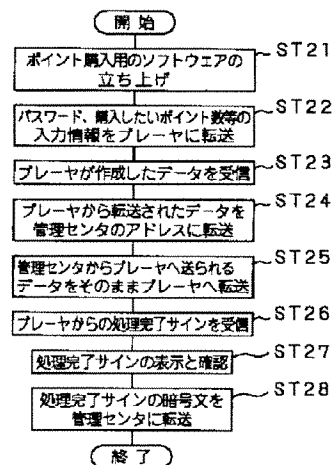


ポイント購入時のプレイヤーのフローチャート

【図3】

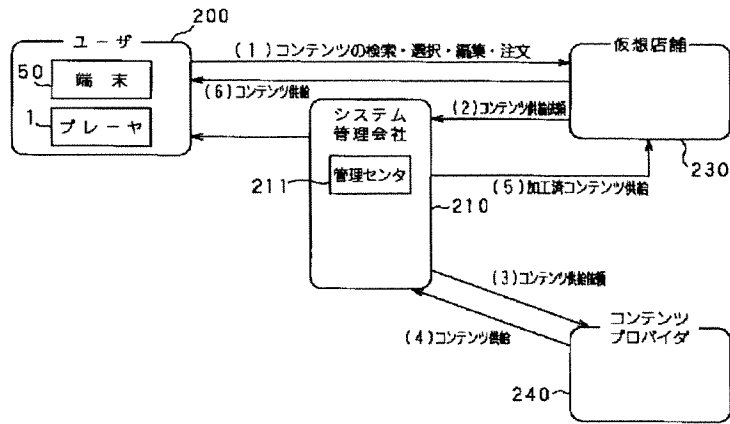


【図9】

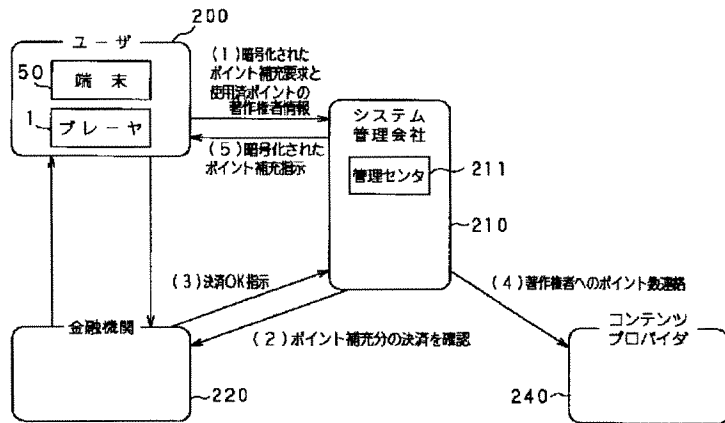


ポイント購入時のユーザ端末のフローチャート

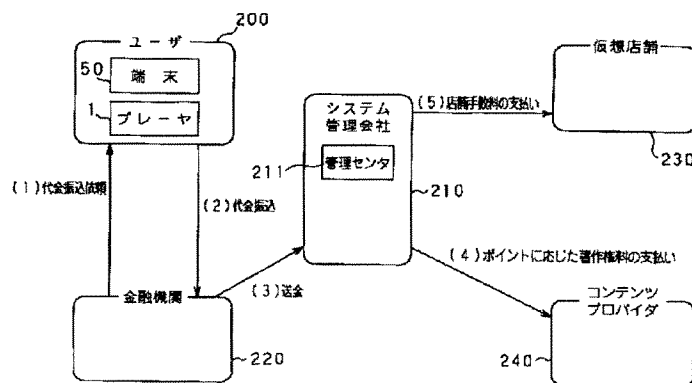
【図5】



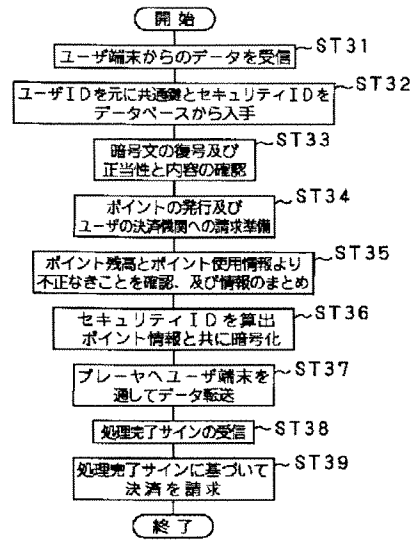
【図6】



【図7】

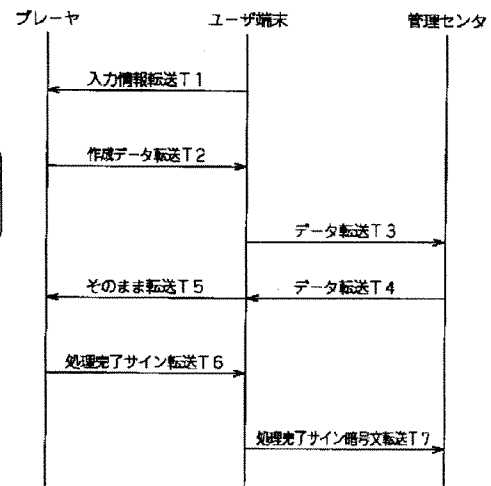


【図10】



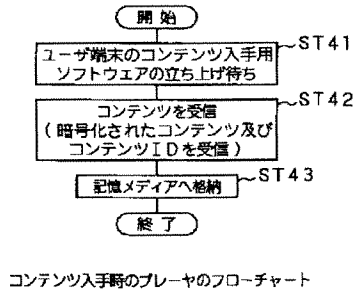
ポイント購入時の管理センタのフローチャート

【図11】

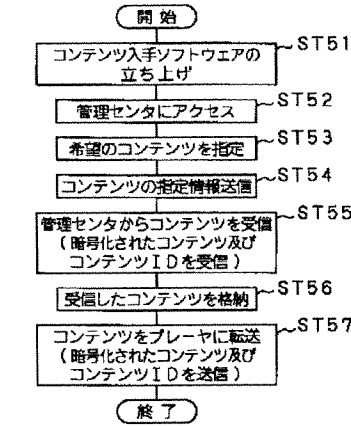


ポイント購入時のシーケンス

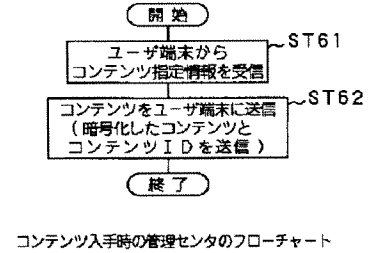
【図12】



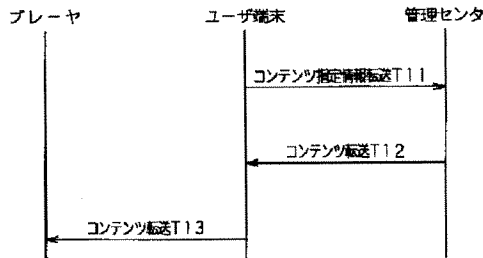
【図13】



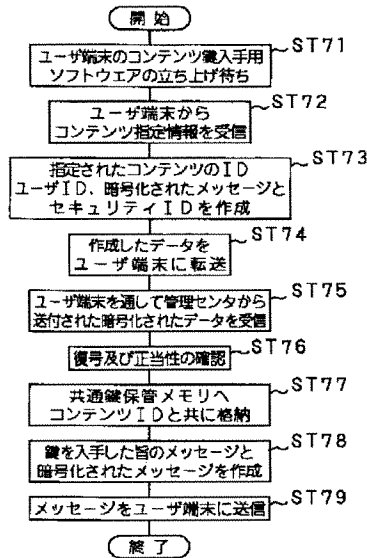
【図14】



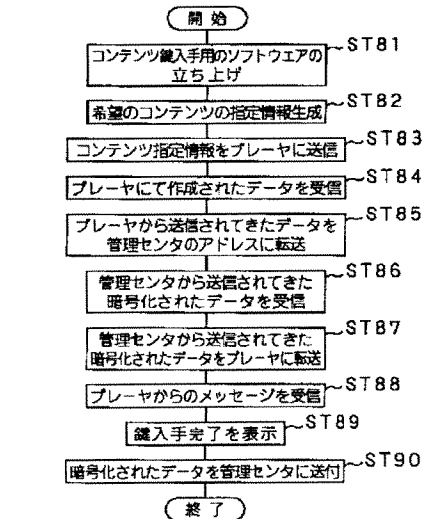
【図15】



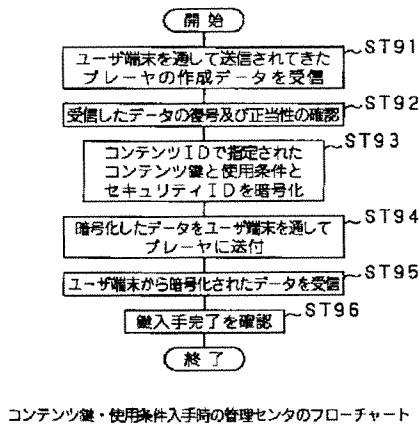
【図16】



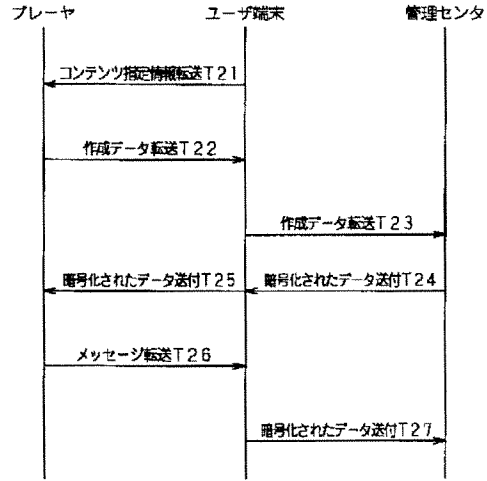
【図17】



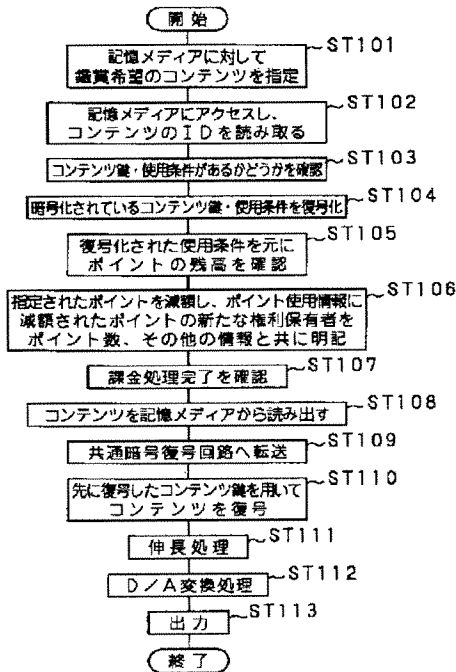
【図18】



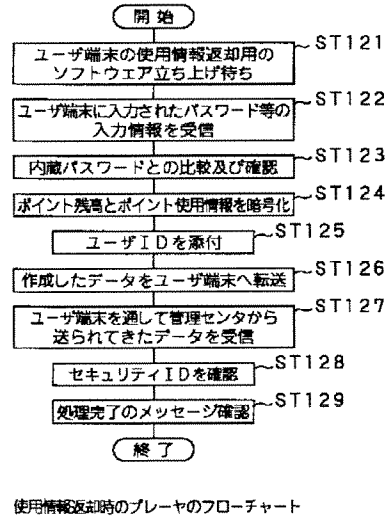
【図19】



【図20】



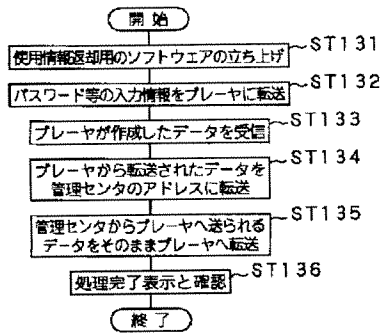
【図21】



コンテンツ鑑賞時のプレイヤーのフローチャート

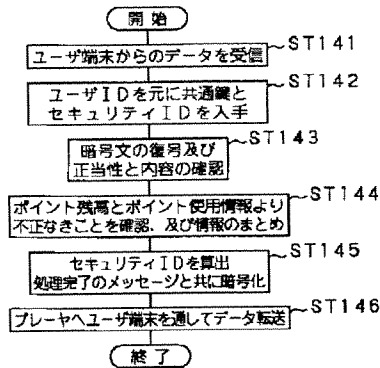
使用情報返却時のプレイヤーのフローチャート

【図22】



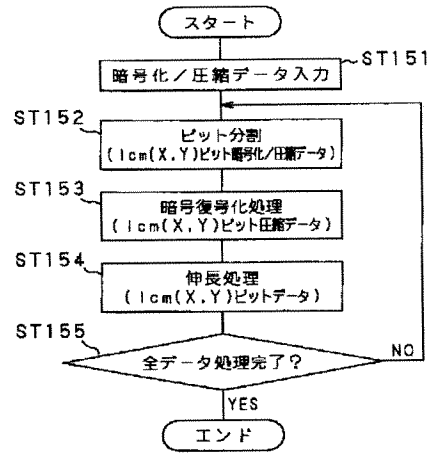
使用情報返却時のユーザ端末のフローチャート

【図23】

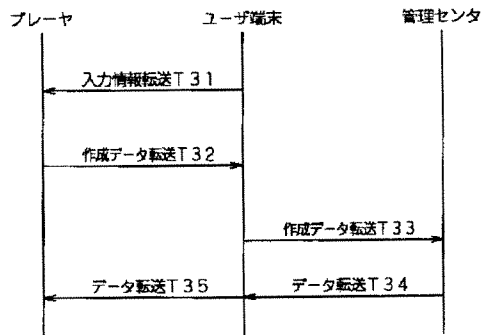


使用情報返却時の管理センターのフローチャート

【図25】

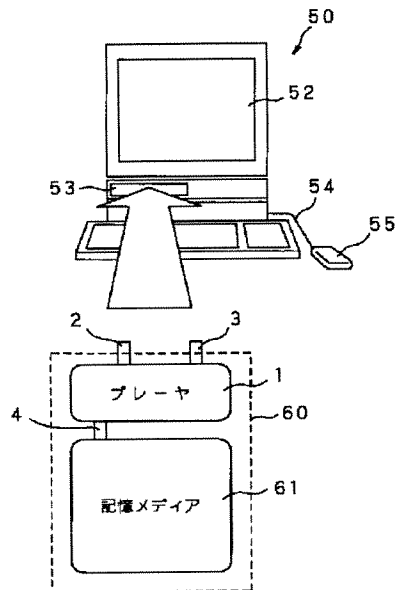


【図24】

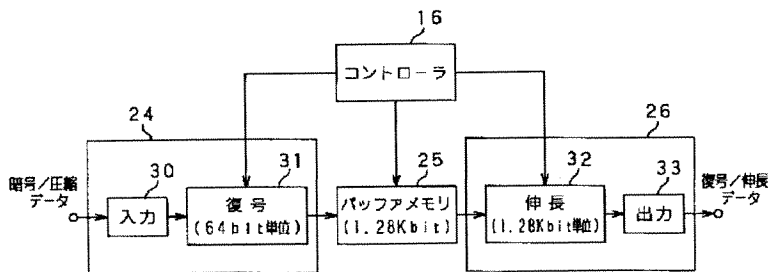


使用情報返却時のシーケンス

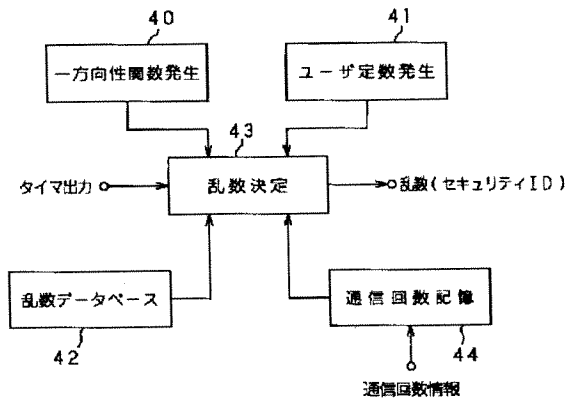
【図39】



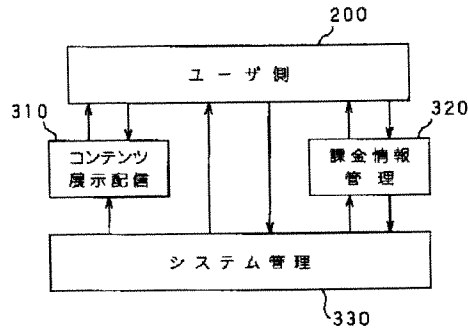
【図26】



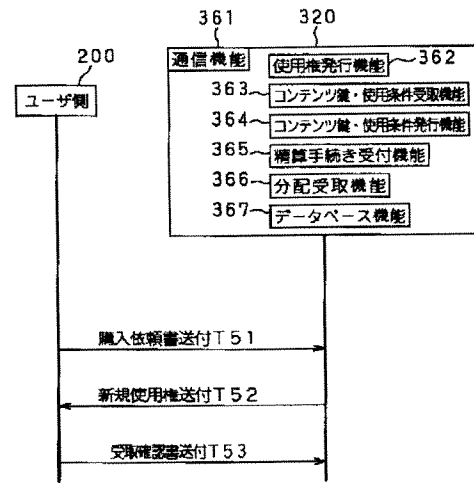
【図27】



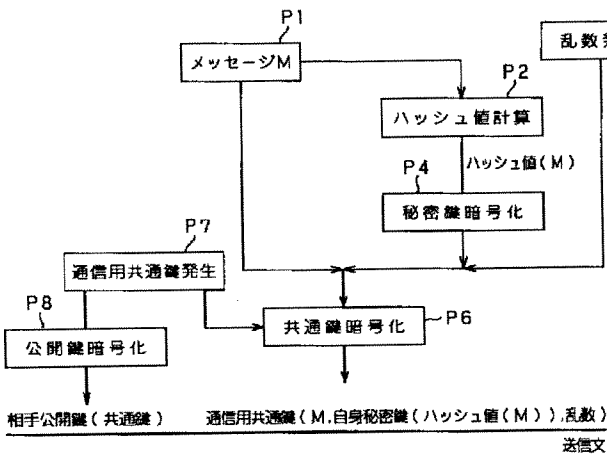
【図30】



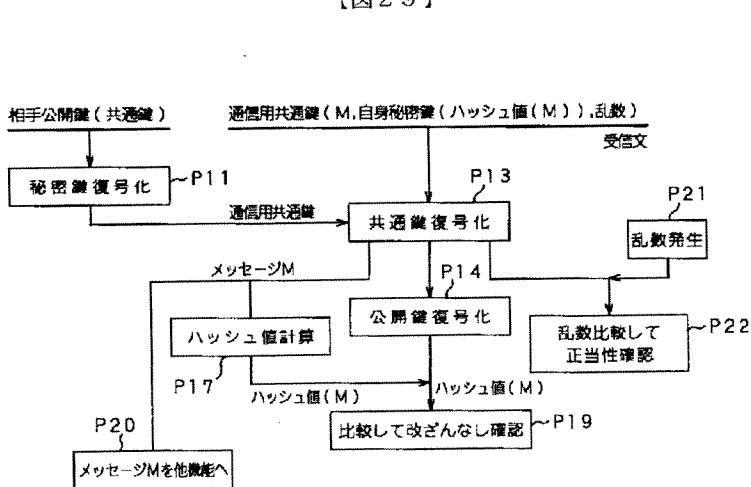
【図32】



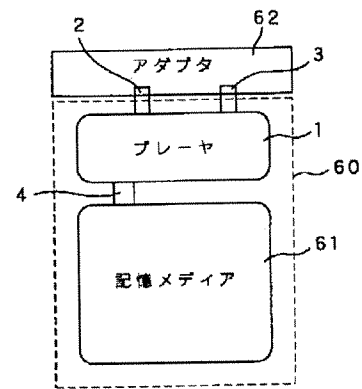
【図28】



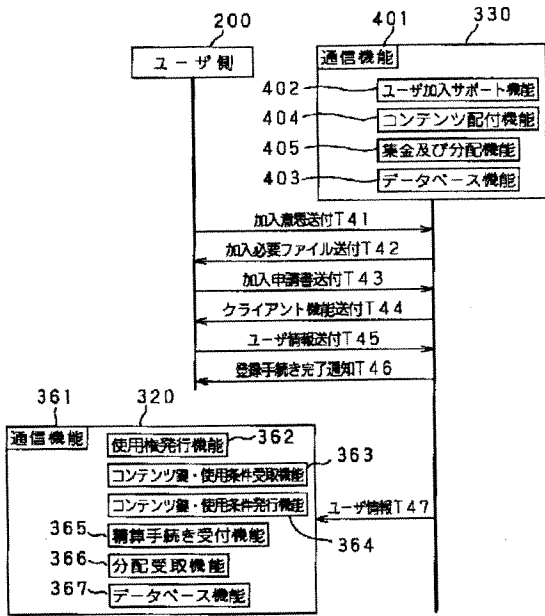
【図29】



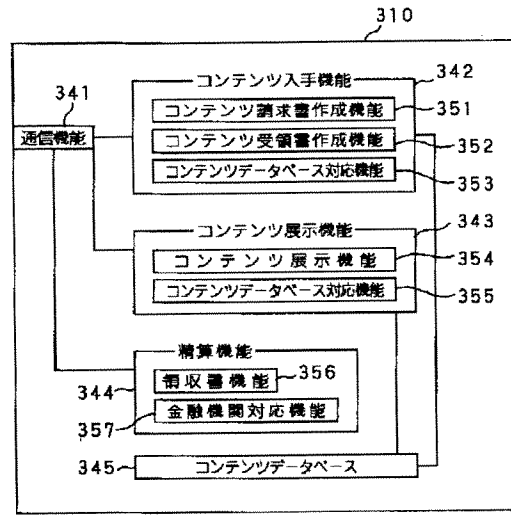
【図40】



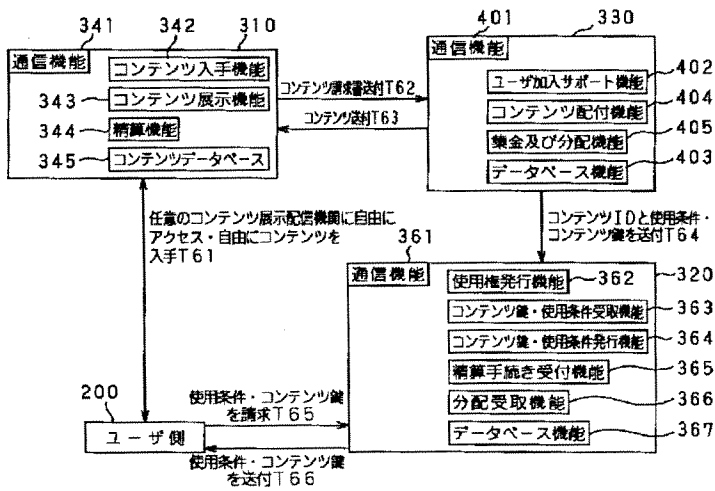
【図31】



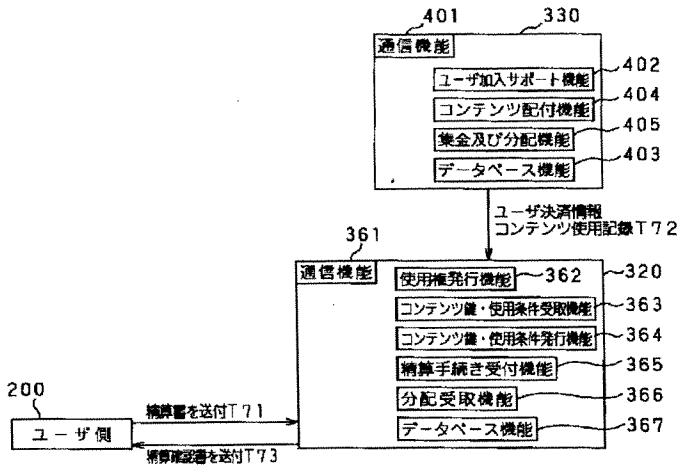
【図35】



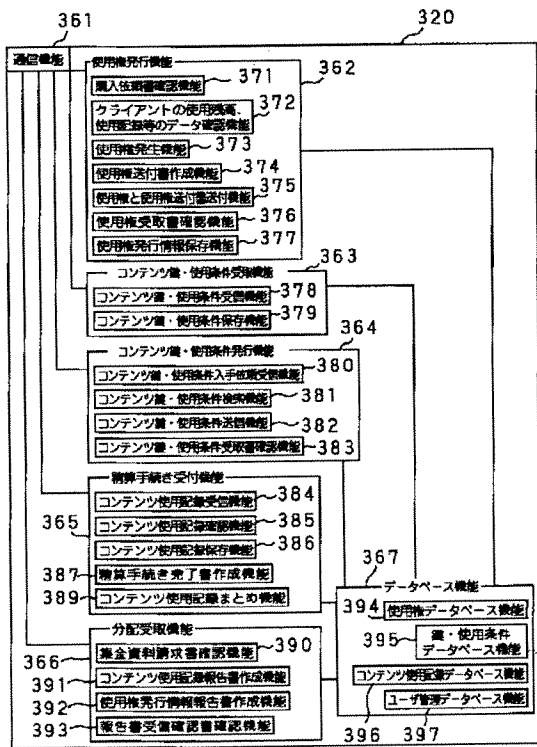
【図33】



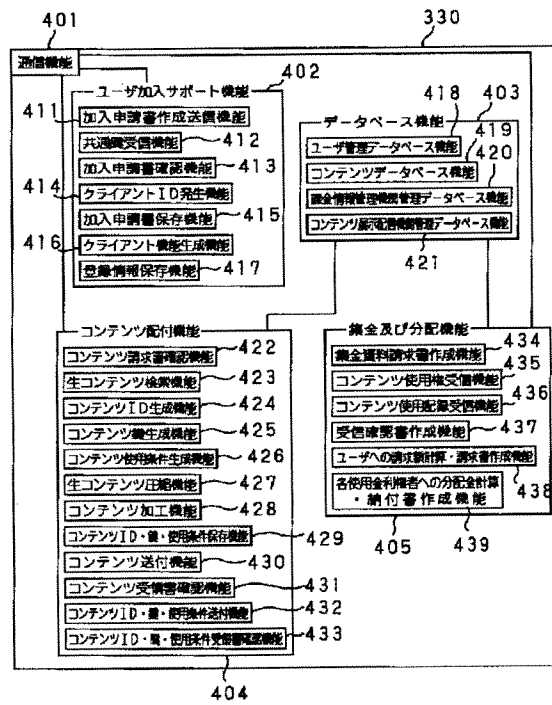
【図34】



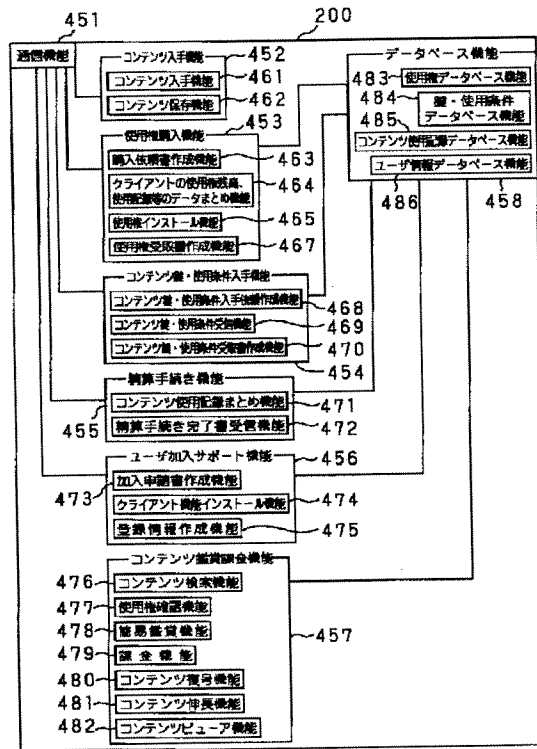
【図36】



【図37】



【図38】



フロントページの続き

(51)Int.Cl.⁵
 H04L 29/08
 // G06F 9/06

識別記号
 550

F I
 H04L 9/00
 13/00

673D
 673B
 307Z